NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USING INFORMATION-SHARING EXCHANGE TECHNIQUES FROM THE PRIVATE SECTOR TO ENHANCE INFORMATION SHARING BETWEEN DOMESTIC INTELLIGENCE ORGANIZATIONS

by

Aaron Kustermann

December 2013

Thesis Advisor:	Christopher Bellavita
Second Reader:	Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2013	Master's Thesis

4. TITLE AND SUBTITLE
USING INFORMATION-SHARING EXCHANGE TECHNIQUES FROM THE PRIVATE SECTOR TO ENHANCE INFORMATION SHARING BETWEEN DOMESTIC INTELLIGENCE ORGANIZATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Aaron Kustermann

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number NPS.2010.0001-IR-EP7-A

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

Security and intelligence organizations have challenges in information sharing have resulted in incomplete information. Since 2001 state and local governments in the United States have formed information sharing hubs called fusion centers which request information from peer fusion centers as well as sharing situation reports about emerging and ongoing security situations. The requests for information (RFI) and situation awareness reporting processes are manual and occur without data standards or process standards. Public sector and private sector information sharing systems utilized both process and data standards to automate routine information sharing between organizations like those exchanges between fusion centers. These standards are coupled with information sharing tools that better enable consumer services, such as searching and booking airline travel through on-line systems, exchanges of criminal justice information using the National Information Exchange Model (NIEM) and sharing of patient and medical information utilizing the Health Information Exchange (HIE).

This thesis combines the process and tools from both the public and private sector's data and process standards and the use of information sharing tools to propose a conceptual national intelligence-sharing model (NISM). SMEs from the intelligence, counterterrorism and technology communities, within the fusion center environment, were used to review, modify, and validate NISM.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Sharing, Intelligence, Technology, Fusion Centers	83
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

USING INFORMATION-SHARING EXCHANGE TECHNIQUES FROM THE PRIVATE SECTOR TO ENHANCE INFORMATION SHARING BETWEEN DOMESTIC INTELLIGENCE ORGANIZATIONS

Aaron Kustermann
Chief Intelligence Officer, Illinois State Police, State of Illinois
B.A., Western Illinois University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2013**

Author: Aaron Kustermann

Approved by: Christopher Bellavita, PhD
Advisor

Richard Bergin
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Security and intelligence organizations have challenges in information sharing have resulted in incomplete information. Since 2001 state and local governments in the United States have formed information sharing hubs called fusion centers which request information from peer fusion centers as well as sharing situation reports about emerging and ongoing security situations. The requests for information (RFI) and situation awareness reporting processes are manual and occur without data standards or process standards. Public sector and private sector information sharing systems utilized both process and data standards to automate routine information sharing between organizations like those exchanges between fusion centers. These standards are coupled with information sharing tools that better enable consumer services, such as searching and booking airline travel through on-line systems, exchanges of criminal justice information using the National Information Exchange Model (NIEM) and sharing of patient and medical information utilizing the Health Information Exchange (HIE).

This thesis combines the process and tools from both the public and private sector's data and process standards and the use of information sharing tools to propose a conceptual national intelligence-sharing model (NISM). SMEs from the intelligence, counterterrorism and technology communities, within the fusion center environment, were used to review, modify, and validate NISM.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

B2B	Business to Business
CAP	Common Alerting Protocol
COP	Common Operational Picture
CPFR	Collaborative Planning, Forecasting, And Replenishment
CRP	Continuous Replenishment Programs
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOI	Department of the Interior
DOJ	Department of Justice
EDI	Electronic Data Interchange
Email	Electronic Mail
EPA	Environmental Protection Agency
EPIC	El Paso Intelligence Center
FBI	Federal Bureau of Investigation
FGDC	Federal Geographic Data Committee
FPS	Federal Protective Service
GAO	Government Accountability Office
GDS	Global Distribution Systems
GJXML	Global Justice Extensible Markup Language
HIE	Health Information Exchange
HITECH	Health Information Technology for Economic and Clinical Health
HSIN	Homeland Security Information Network
HSIN-Intel	Homeland Security Information Network Intelligence
IC	Intelligence Community
iCAV	Integrated Common Analytical Viewer
ISE	Information Sharing Environment
JITF-CT	Joint Intelligence Task Force-Combating Terrorism
LEO	Law Enforcement Online
MLS	Multiple Listing Services

NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
N-DEx	National Data Exchange
NIEM	National Information Exchange Model
NISM	National Intelligence Sharing Model
NPS	Naval Postgraduate School
NSIS	National Strategy for Information Sharing
PHDSC	Public Health Data Standards Consortium
POP3	Post Office Protocol 3
POS	Point of Sale
RETS	Real Estate Transaction Standard
RFC	Request for Comment
RFI	Request for Information
SME	Subject Matter Experts
SMTP	Simple Mail Transfer Protocol
STIC	Statewide Terrorism and Intelligence Center
THN	Tourism Harmonisation Network
VCC	Virtual Command Center

ACKNOWLEDGMENTS

I would like to open with thanking my wife, Annie, who was amazing through this process and always reassured me. You are far smarter than I will ever be and your advice and guidance made this journey possible. I love you and appreciate your support today and every day. My mother Sue Ellen was an educator before starting a family and always taught my brothers and I the value of an education. For this, I am grateful.

I would like to thank the incredible faculty, staff, and associates of the Naval Postgraduate School for the dedication to the students they serve. This program has forever changed my way of thinking and will certainly alter my career and life in positive ways. My cohort, 0801/0802, made this experience amazing and each of you contributed to my thinking. In addition to being thesis advisors, these two professionals are also wonderful mentors. Professor Bergin and Doctor Bellavita you challenged me in ways I cannot express and I hope someday to know a fraction of what you have learned about people and science. I came to this program knowing it would be a challenge and left the program wishing I could do it again and again.

Many friends and co-workers encouraged me and kept our operations running while I was busy learning. To David Waldrop, Pat Duecy, Bart Johnson and Van Godsey, thank you for participating in this thesis project and sharing your ideas and thoughts. The men and women of the national fusion center community and the Illinois State Police are awesome and I would put you up against any challenge. Colonel Rob Haley, Lieutenant Colonel Todd Kilby, Major Brad Carnduff, Lieutenant Eric Wolf, Master Sergeant Mike Gillock, Criminal Intelligence Analyst Tim Harney, Master Sergeant Calvin Brown, Public Service Administrator Dora Tyrrell and Trooper Mark Beagles, I thank you for supporting me and this program in the midst of the public safety challenges we were negotiating. You are the reason I love coming to work everyday and should be held up as examples of what it means to be public servants. Lastly, to my

carpool. First Deputy Director Charles Brueggemann, Lieutenant Colonel Craig Koehler, and Major Jay Keeven, you are great professional and personal examples for me and I miss our years commuting together as much as I miss the NPS experience. First Deputy, I had this experience because of your influence and insistence, and for that, and hundreds of other reasons, I will always be grateful.

This work is dedicated to my son, August Richard Kustermann, and my father, Richard Royce Kustermann. Dad, you taught me the work ethic and diligence necessary to do anything. August, you are brilliant and one day you will write something that exceeds this work and any expectation Annie and I have for you.

I. INTRODUCTION

A. PROBLEM STATEMENT

Inter-organizational information sharing between and amongst local, state and federal agencies is necessary to ensure the security of the United States. As discovered by the 9/11 Commission, many local, state and federal agencies failed to share information on a regular basis (National Commission on Terrorist Attacks, 2004). While the 9/11 Commission was conducting its study, states and urban areas were already forming fusion centers, which later came to be the decentralized network the Commission recommended in its 2004 report. Fusion centers are to serve as information-sharing mechanisms for public safety personnel from local, state, and federal agencies. Today, every U.S. state and several urban areas have formed fusion centers. In 2007, the White House published the *National Strategy for Information Sharing*, which concluded "state and major urban area fusion centers represent a valuable information-sharing resource and should be incorporated into the national information-sharing framework" (National Strategy for Information Sharing, 2007, p. 3). Additionally, the White House builds on the Commissioners' recommendation, and in 2010, with the National Security Strategy, and in 2012, with the National Strategy for Information Sharing and Safeguarding by calling for leveraging the information provided by the national network of fusion centers (The White House, 2010, 2012).

Fusion centers are defined for this work as the 77 state and local coordinated information and intelligence centers, as well as the federally coordinated mission-specific intelligence centers, such as the National Counterterrorism Center (NCTC), El Paso Intelligence Center (EPIC), and others. These centers utilize the intelligence cycle to process information on many types of criminal activity ranging from property crimes to terrorism. The intelligence cycle (Figure 1), as defined by the *National Criminal Intelligence Sharing Plan*, is

comprised of six processes: (1) planning and direction, (2) collection, (3) collation or processing, (4) analysis, (5) dissemination, and (6) reevaluation (U.S. Department of Justice, 2005).

Figure 1. Intelligence Cycle—National Criminal Intelligence Sharing Plan (From U.S. Department of Justice, 2005)

The collection, collation, and dissemination steps are performed several times each day by local, state, and federal fusion centers that routinely exchange information with one another. The analysis step is designed to interrogate further the information and refine the conclusions and impacts. Also, in the analysis step, information reliability judgments can be considered. The collection and collation steps rely on Request for Information (RFI) processing, and the dissemination step is partially completed through sharing information on emerging or on-going situations or events. These daily steps are performed and processed without universal guidelines, standards, or protocols. The following is

an example of an Illinois RFI, which illustrates how the process works today and how today's processes can lead to missing or overlooked information and requires significant personnel resources to complete.

1. Today's RFI Process

Investigators in a narcotics task force who are performing a search warrant at a residence where narcotics were being distributed initiate an example of a routine RFI in Illinois. The mobile telephone of the target of the investigation is seized (under the proper legal guidelines) and reviewed for evidentiary and intelligence value. The target's telephone contains names and associated telephone numbers with area codes throughout the country. A message is sent from the narcotics task force investigators to the Illinois fusion center, called the Statewide Terrorism and Intelligence Center (STIC), requesting further information on these names and telephone numbers. The STIC then sends a RFI to other state fusion centers associated with those area codes. This RFI is likely communicated using electronic mail (Email), is comprised of unstructured text, contains some background information on the investigation, and requests fusion centers to comply with a specific request. This Email is sent to a general fusion center Email in-box and is processed by fusion center personnel. Generally, the answering fusion center will reply to the original Email, containing the RFI, with any information available from their resources. An analyst or officer at the STIC combines all the information received from the other fusion centers (collation), and removes any redundant information. Once the collation process is completed, the analyst begins to analyze the resulting data. The collection and collation process could take an hour or days depending on the volume of information requested and the number of organizations involved in the original RFI, other requests or reports coming into the STIC, or incidents occurring in the other jurisdictions. Each center handles these RFIs differently and constructing the national answer about a target of an investigation is time consuming. The STIC processes more than 30,000 RFIs a year and rely on responses to these

RFIs for the majority of the requests processed. Collating the results of these 30,000 RFIs is generally performed using word processing software.

2. Sharing Information during Emerging Incidents

One of the core missions of a fusion center is to share information during emerging or on-going situations or events. The national network of fusion centers relies on information from the other centers during emerging situations to assess the impact on their geographical area and to have situational awareness. During emerging situations, the information can be scarce, incorrect, and dynamic for hours or days. Often early situational reporting during emerging incidents is incorrect. Today, the process for sharing information during emerging situations is similar to that of the RFI. This fictional example will illustrate the process during a mass causality situation.

The Illinois STIC has learned of a shooting at a place of worship in Illinois. STIC personnel would gather as much information as possible about the event from public safety and publically available sources to include internal reporting in databases or systems available to the STIC personnel, as well as open sources, such as the news media. As soon as possible, a STIC staff member sends an Email to the other fusion centers' Email accounts throughout the nation. This message would include the date and time of occurrence, location, numbers of victims, location and type of place of worship, time, date and current situation, a narrative of the situation, and possibly, the classification, source, and handling instructions for the information. As the STIC learns more about the subject, future messages are issued in the same fashion correcting or updating the previous message. The STIC has flexibility in how it shares the information and can choose what information to share, how the information is shared, with what organizations it is shared, and other variables. Likewise, the STIC can choose to issue updates whenever it prefers to do so, or for that matter, not issue an update at all.

The fusion center inter-organizational work that has been done has blocked the creation of intelligence web-portals or online libraries of finished or final intelligence products. Some of these efforts have been successful, such as the Homeland Security Information Network Intelligence (HSIN-Intel), but even HSIN-Intel stops short of creating a national RFI network or shared situational awareness. To date, fusion center information sharing efforts have used federally driven, top-down models in which the fusion center must adopt a particular federal system or network. This practice requires the 77 state and local fusion centers to adopt each of the federal agencies' systems, which results in redundant reporting and inefficiency.

B. RESEARCH QUESTION

How can existing public and private sector mechanisms be used to enhance domestic information collection, collation or processing, and dissemination?

Specifically, how can existing technical processes, tools, and data standards from the public and private sectors enhance domestic information collection, collation or processing, and dissemination?

C. HYPOTHESIS ARGUMENTS

This work proposes the creation of data and process standards to create a single act of publication and collation for requesting information and sharing information about on-going situations. The sender would use an established template for dissemination and responding to national RFIs and a similar template for sharing information during an emerging situation. The recipient would subscribe to these standardized feeds of information to enable recipient IT systems to route, filter, and process the information according to their mission and needs. Responses would be guided by similar standards to enable threaded display and automated collation.

1. Improvements to Request for Information (RFI) and Situational Awareness Reporting

The current RFI and shared situational awareness processes between intelligence organizations in the United States can be improved by leveraging the lessons learned and work done in the private sector with regards to business to business (B2B) collaborative techniques. Similar B2B collaborations exist in continuous replenishment programs (CRP) and electronic data interchange (EDI), wherein two firms have pre-established information sharing arrangements. These arrangements exist within inventory and ordering systems and are used by large U.S. retailers to exchange information with product suppliers (Lefebvre, 2003). Connecting systems in this manner would eliminate the present need for manual interpretation at each fusion center upon the receipt and dispatch of information and would allow for a more efficient process overall by allotting more time for the analysis of collated materials and providing a more comprehensive collection of materials.

The RFI process is similar to an inventory linkage, wherein one system is asking another a question. In the case of a fusion center, a national query or RFI would be published using standard fields derived from the National Information Exchange Model (NIEM). This RFI would trigger a query in the other fusion center's intelligence systems and automatically supply a response. These RFIs, and the replies or responses, would require an establishment of standard data fields. Each fusion center would not need to adopt a national system, but instead would use the intelligence systems they currently employ and publish the RFI to the national standard.

Using the same principles, government organizations can share information about emerging and on-going situations with others involved or interested organizations far more efficiently. Like the RFI process, each center would use its own system to report situations, and this dynamic exchange would be digested by each organization to create national shared situational awareness.

2. Significance of Research

This research will contribute to the literature resources available to domestic intelligence policy makers, as well as many organizations and communities of interest. These interested organizations consist of the federal intelligence community, the federal law enforcement, and intelligence gathering and analysis organizations, the Director of National Intelligence, the state and local fusion center community, intelligence analysts and officers, and government technology contractors. The findings and recommendations pursuant to this research provide policy makers, planners, and technology experts with a partially vetted concept, with considerations, and challenges for implementation. Lastly, a partial implementation is underway and at the end of this work. a summary of the current status is outlined.

D. CHAPTER OVERVIEW

This work examines the literature available regarding both public and private sector information sharing systems and yields a conceptual model (the National Intelligence Sharing Model or NISM) for processing RFIs and sharing situation reports. Outlined in the current literature (Chapter II) are the data standards, process standards, and information sharing tools used in the private and public sectors that are then examined for fit within state and local fusion centers.

Chapter III explains the method utilized for vetting the model wherein four subject matter experts (SMEs) were interviewed. These experts were asked about what standards, automated processes, and tools are available to enhance information exchanges. Additionally, they were asked to evaluate the challenges of implementing the NISM, and what these efficiencies in RFI processing and situation reporting would bring in the way of additional time available towards strategic intelligence. Those interviewed raised additional issues to be investigated upon future research. Chapter IV takes into consideration the expert

responses to the conceptual NISM, and proposes changes or alterations to the conceptual NISM. The findings, conclusions, and recommendations are summarized in Chapter V.

II. LITERATURE

Information sharing, including inter-organizational information sharing, has been accomplished by private and public organizations alike. Inter-organizational information sharing is enabled by several factors, three of which are data standards, process standards, and information sharing tools. The following outlines examples of each of these in both private and public organizations.

A. PUBLIC SECTOR INFORMATION SHARING

The Government Accountability Office (GAO) report from April 2007 concludes 17 major information-sharing networks are in use by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) (U.S. Government Accountability Office, 2007). Additionally, these networks cost $893.1 million to operate in 2005 and 2006. Many of these networks are used for in-house communications and are not available to other organizations or communities. Two networks are available to federal, state and local communities: the Homeland Security Information Network (HSIN), and the Law Enforcement Online (LEO). Each portal, as they are commonly called, creates national web-based libraries for sharing finished intelligence products. The HSIN is operated by the DHS, and LEO is operated by the DOJ. Other networks are emerging in the information-sharing space from the DHS Federal Protective Service (FPS), and the Federal Bureau of Investigation's (FBI's) e-Guardian program. In 2011, the GAO recommended an information-sharing environment (ISE) for the exchange of terrorism-related information (Larence, 2011).

1. Homeland Security Information Network (HSIN)

The HSIN brand is divided into two parts, HSIN and HSIN-Intel. The larger HSIN is devoted to information sharing amongst the public safety community, which includes law enforcement, emergency management, critical infrastructure, and others. The HSIN-Intel program serves the state and local fusion center community. Both programs are web-portals with document libraries and

embedded communication capabilities. The portals are searchable, and in the HSIN-Intelligence portal, advanced storage abilities exist to limit document audience. In addition to document sharing, as well as secure messaging and chat, other features are also available. The HSIN offers a situational awareness tool called the Common Operational Picture (COP), has integrated mapping capability through the Integrated Common Analytical Viewer (iCAV), and utilizes Adobe Connect software for facilitating real-time meetings and collaboration. The HSIN program costs approximately $21 million to operate annually (U.S. Government Accountability Office, 2008). In May 2013, the HSIN program transitioned to what is called HSIN Release 3 or HR3. This system made technological and user interface improvements, as well as included a secure messaging capability for the HSIN-Intelligence user base (Office of Inspector General, 2013).

2. Law Enforcement Online (LEO)

The major initiative in the DOJ for information sharing is LEO, which operates similar to HSIN and provides some of the same functionality by offering secure messaging and mission specific online portals for communities of interest to post information. LEO's encryption package is used to verify users of other systems, such as National Data Exchange (N-DEx), and operational law enforcement deconfliction systems. In addition to web-portals, LEO offers encryption for access to the national deconfliction network (RISSSafe) and Virtual Command Center (VCC), which is a web-based incident management tool (U.S. Government Accountability Office, 2007).

The 9/11 Commissioners recommended that the President be responsible for coordinating issues to ultimately "create a trusted information network" (National Commission on Terrorist Attacks, 2004, p. 418). In August 2004, the President issued *Executive Order 13356* that directed federal organizations to give information sharing and counter-terrorism the highest priority. *Executive Order 13356* also provided direction to federal entities to share information with

state and local authorities. It specifically directed the Intelligence Community (IC) to create intelligence reports and summaries at the classification level to be accessible by the state and local jurisdictions. The National Strategy for Information Sharing (NSIS) builds on the concept above, and charges state and local fusion centers with establishing protocols to handle bi-directional situational awareness reporting to local jurisdictions, the private sector, and the federal government (National Strategy for Information Sharing, 2007). The 2010 National Security Strategy stresses timely information exchanges and suggests the development of the national fusion center network should be further leveraged (The White House, 2010). This strategy proposes an "integrated approach to information systems" through "collaboration across government" (The White House, 2010, p. 51).

Following 9/11, U.S. government organizations were given clear direction and legislative authorities. These new strategies and laws created several organizations and systems designed to improve information sharing. Additionally, the leaders of government agencies were directed to make information sharing a priority and to create protocols and formalized processes for sharing information with state and local partners.

B. PRIVATE SECTOR INFORMATION SHARING

Some private sector firms have accomplished inter-organizational information sharing as well. Participating organizations use several mechanisms to share information. These mechanisms allow firms to share real-time information about issues ranging from ordering and reordering, as well as inventory levels to other logistics, such as delivery dates, shipment locations, and details about transportation.

The private sector uses B2B collaboration techniques to facilitate transactions between organizations. Examples of these transactions include, ordering and reordering, invoicing and payments, and shipping and logistical exchanges. These transactions are routine and inter-organizational information

sharing can enable the automation of work (Barratt, 2004). Technologies allow firms to collaborate electronically and automate exchanges, which previously required human attention (Attaran & Attaran, 2007). Some forms of B2B collaboration are called CRP, EDI and collaborative planning, forecasting, and replenishment (CPFR).

CRP represent inter-organizational information sharing, wherein two firms' systems tightly collaborate. One example of a CRP system is the reordering process between a retailer and wholesaler. The two firms' inventory and ordering systems are linked and these systems automatically share information and act upon pre-defined rules. Once the first order has been placed, terms agreed upon, and the inventory and ordering systems linked between firms, the CRP is automatically sharing information and the replenishment or reordering of the item is performed, (Attaran & Attaran, 2007)which is an example of tightly coupled collaboration between firms.

An information broker between firms enables information sharing using EDI techniques. By using an EDI, firms are able to share invoices, inventory levels, and other information by publishing the information (using data standards) to a service shared by both firms. For example, one firm places an order using its internal system, the order is transmitted to the EDI, and it routes the order to the seller. EDI, fueled by the Internet, has continued to improve and become economically beneficial (Attaran & Attaran, 2007). EDI techniques in public health settings have proven efficient in exchanging information (U.S. Government Accountability Office, 2010). The EDI used by a U.S. State Department of Public Health provided immediate access to condition information and supported early detection of H1N1 cases and was valuable (U.S. Government Accountability Office, 2010). Figure 2 illustrates the EDI model for information sharing in a public health and medical environment. This model makes use of data standards and process standards to facilitate the timely and efficient exchanges of health information between health care providers.

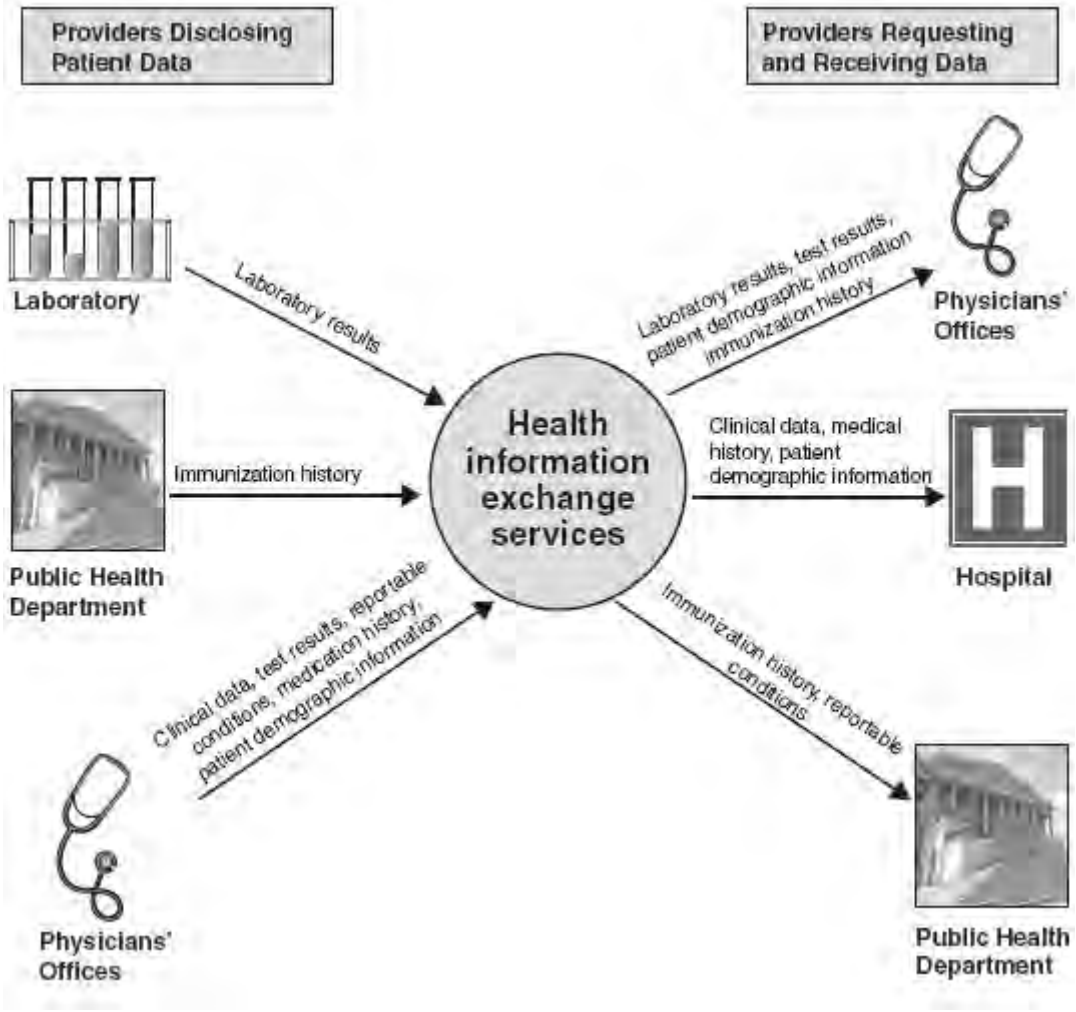


Figure 2. Health Information Exchange Model (From U.S. Government Accountability Office, 2010, p. 6)

CPFR is an example of advanced inter-organizational information sharing. Whereas EDI and CRP focus on automating repeating functions, in a CPFR situation, several parts of the supply chain are part of the collaboration. CPFRs enable information sharing on inventory, point of sale data, promotions, orders, shipments and production, and sales forecasts. These systems enable information sharing from the early stages of inter-firm arrangements to the sales and replenishments phases.

The private sector relies on B2B collaboration techniques to share information between firms. These techniques include connecting firms to

automate a singular piece of work between them, using inter-organizational services to link firms together, and sharing information throughout several phases of supply chain process. These programs are designed to enable information exchanges inside supply chains where prearranged rules (price, packaging and others) exist (Attaran & Attaran, 2007).

C. PRIVATE SECTOR DATA STANDARDS

Information sharing in private and public organizations, in some circumstances, relies on common data standards. Researchers Cirincione and Bacharach (2007) state, “data standards represent agreement” (, p. 136). These agreements enhance information exchanges by creating an agreed framework in the way of data fields and labels. Ciricione and Bacharach (2007) summarize the need to create data standards in the private sector as follows:

> When different companies use similar data field naming conventions to handle the same type of information, they are freed from the requirement to develop costly, dedicated data conversion systems in order to interface with other businesses in the same industry. Such interfacing has become a priority in the industry as its continuing integration with the public capital markets has increased the pressure for rapid, consistent, and accurate transfers of data. (p. 129)

Private sector firms have created standards in many business markets, including health care, real estate, and travel industries, to enable and enhance inter-organizations information sharing.

The health and medical communities employ the Public Health Data Standards Consortium (PHDSC), which has created data standards for many exchanges involving health care information. Seventeen data standards create uniformity in data ranging from hospital bed availability to payer typology. One such standard in the medical community is used for uniform billing. The health and medical communities, and specifically, health care providers and payers, use this standard, named UB-92 (seen in Figure 3), for processing health care claims (American Hospital Association, 2009). The patient or client completes the form

for the health care provider and the information necessary to process the payment is shared with the claims organization, the provider, the insurance industry, and other relevant parties. The Health Information Exchange (HIE) provides similar standards in support of the Health Information Technology for Economic and Clinical Health (HITECH). The HITECH creates a standards-based electronic exchange of health and patient information for use by private (hospitals, health care providers, and physicians) and public organizations (public health agencies) (Department of Homeland Security, Office of Inspector General, 2013). Incentives in the form of grant opportunity and claims of efficiencies are designed to attract the public and private organizations' participation (U.S. Governmental Accountability Office, 2010).

UB92 Claim Form

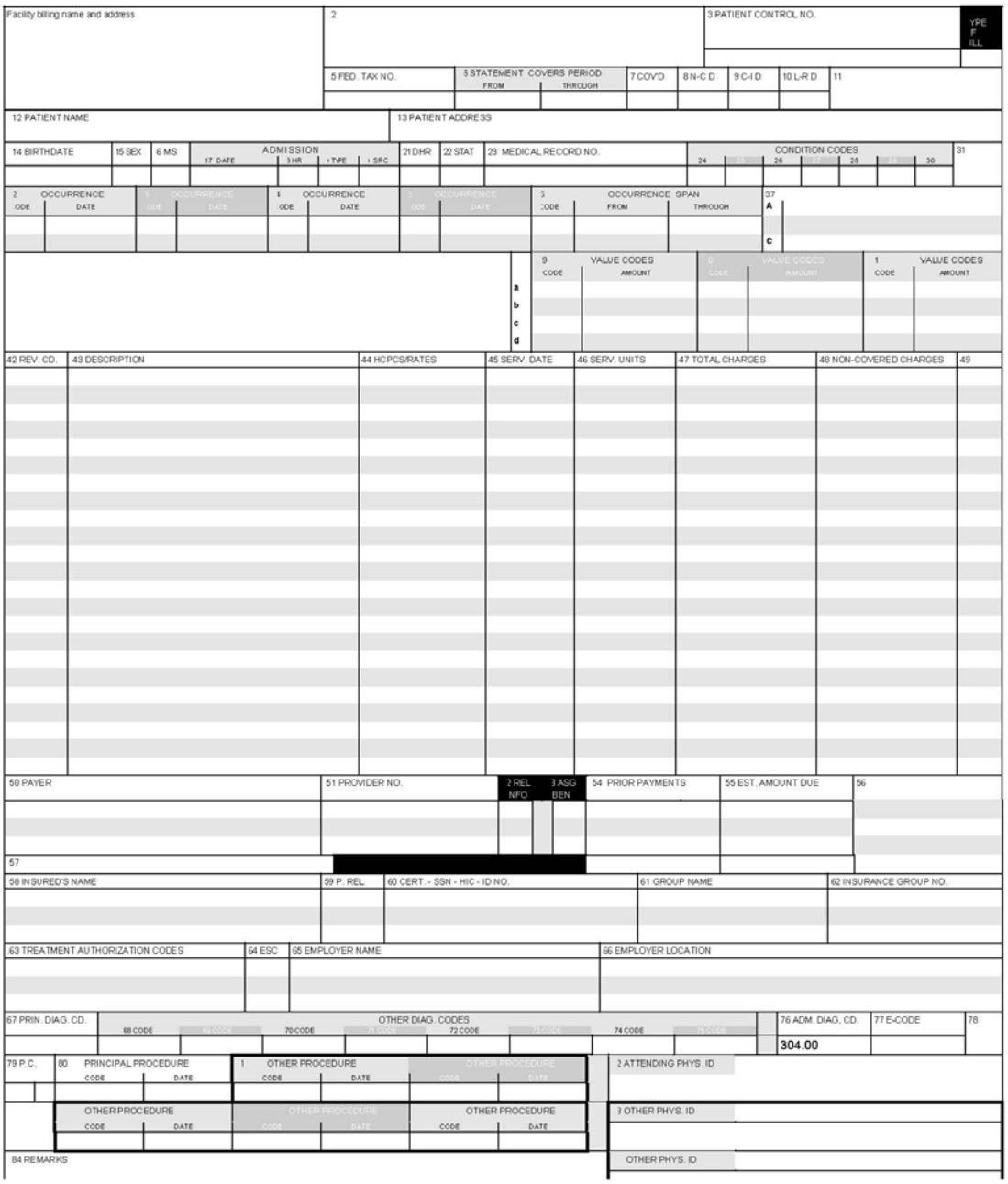


Figure 3. UB92 Claim Form (From National Uniform Billing Committee, n.d.).

Similar standards exist in the real estate industry. Like other enterprises, the real estate industry does not stand alone. Realtors, lenders, appraisers, titling organizations, insurance companies, and others rely on information shared between one another. Inter-organizational information sharing in these industries

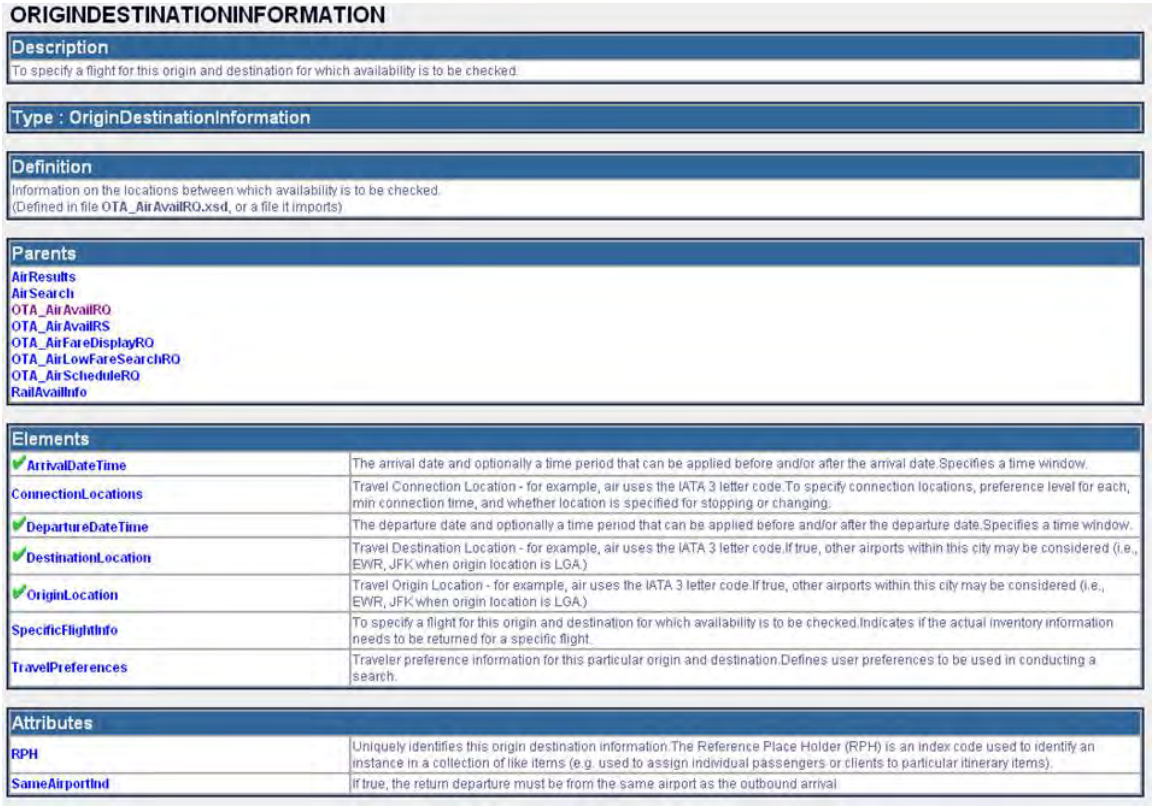
also relies on data standards. The Real Estate Transaction Standard (RETS) provides these standards for the real estate industry. One such standard provided by RETS enables inter-organizational information sharing between realty firms and multiple listing services (MLS). For instance, when using data standards in RETS, realtors can upload a new listing or edit an existing listing using their individual system and export a listing to an affiliated MLS (Real Estate Transaction Standard, 2009). The RETS utilizes 140 common fields (shown partially in Figure 4) used by many of the more than 800 MLSs (National Association of Realtors, 2007).

StandardName	Element	Attribute	Type	Value	Description
School.Primary	Primary		Text		The name of the primary school having a catchment area that includes the associated property.
School.JrHigh	JrHigh		Text		The name of the jr high school having a catchment area that includes the associated property.
BedRoom	BedRoom		Container		Information about specific bedrooms within a single-family property or a single unit of a multi-family property
BedRoom.Master	MasterBedroom		Container		The Geometric description of a Master Bedroom within a single-family property or a single unit of a multi-family property. The definition of a master bedroom is determined by local custom.
BedRoom.Master.Indicator		Indicator	Enumeration	Unknown	Unknown indicates that neither condition (Yes or No) can be determined.
				Yes	Indicates that this feature does exist.
				No	Indicates that this feature does not exist.
BedRoom.Master.Dimensions	Dimensions		Text		The room dimensions. This SHOULD be expressed as a text string consisting of one or more numeric quantities giving the linear distance between vertices of the polygon enclosing the space and separated by white-space and the letter "x".
BedRoom.Master.Length	Length		Numeric		The rooms length. Represented as a number.
BedRoom.Master.Length.Units		Units	Enumeration	Feet	The length is expressed in feet.
				Meters	The length is expressed in meters
				Acres	The length is expressed in acres.
				Hectares	The length is expressed in hectares
BedRoom.Master.Width	Width		Numeric		The rooms width. Represented as a number.
BedRoom.Master.Width.Units		Units	Enumeration	Feet	The length is expressed in feet.
				Meters	The length is expressed in meters
				Acres	The length is expressed in acres.
				Hectares	The length is expressed in hectares
BedRoom.Master.Area	Area		Text		The rooms geometric area expressed in the given units. Numeric areas are preferred; the "TEXT" unit is deprecated.
BedRoom.Master.Area.Units		Units	Enumeration	SqFeet	An area measurement specified as per SqFeet.
				SqMeters	An area measurement specified as per SqMeters.
				Acres	An area measurement specified as per Acres.
				Hectares	An area measurement specified as per Hectares.
BedRoom.Master.Area.Type		Type	Enumeration	Integer	The area is expressed as an integer number of units
				Float	The area is expressed as a floating point number.
				Text	The area is expressed as a text string that can not be usefully interpreted as a number.

Figure 4. RETS common fields (From Real Estate Transaction Standard, 2009)

The travel industry is a third example of a dependent supply chain of private firms in which data standards are involved in information sharing. Individual customers, travel agencies, lodging and transportation providers, as well as their supply chains, rely on the information shared between firms. This sharing is best observed in the use of on-line travel tools when passengers personally search for their preferred itinerary. Data standards enable these

exchanges and standards organizations like the OpenTravel Alliance (OpenTravel, 2009b), which have aided in their creation. The OpenTravel standards enable inter-organizational information sharing, as well as enhance end user or point of sale (POS) capabilities. The OpenTravel standards are used to carry tens of millions of messages between firms each day (OpenTravel, 2009b). Figure 5 shows the OpenTravel data standard for air travel flights when origin and destination are available.



ORIGINDESTINATIONINFORMATION

Description

To specify a flight for this origin and destination for which availability is to be checked.

Type : OriginDestinationInformation

Definition

Information on the locations between which availability is to be checked.
(Defined in file **OTA_AirAvailRQ.xsd**, or a file it imports)

Parents

AirResults
AirSearch
OTA_AirAvailRQ
OTA_AirAvailRS
OTA_AirFareDisplayRQ
OTA_AirLowFareSearchRQ
OTA_AirScheduleRQ
RailAvailInfo

Elements

✔ArrivalDateTime	The arrival date and optionally a time period that can be applied before and/or after the arrival date.Specifies a time window.
ConnectionLocations	Travel Connection Location - for example, air uses the IATA 3 letter code.To specify connection locations, preference level for each, min connection time, and whether location is specified for stopping or changing.
✔DepartureDateTime	The departure date and optionally a time period that can be applied before and/or after the departure date.Specifies a time window.
✔DestinationLocation	Travel Destination Location - for example, air uses the IATA 3 letter code.If true, other airports within this city may be considered (i.e., EWR, JFK when origin location is LGA.)
✔OriginLocation	Travel Origin Location - for example, air uses the IATA 3 letter code.If true, other airports within this city may be considered (i.e., EWR, JFK when origin location is LGA.)
SpecificFlightInfo	To specify a flight for this origin and destination for which availability is to be checked.Indicates if the actual inventory information needs to be returned for a specific flight.
TravelPreferences	Traveler preference information for this particular origin and destination.Defines user preferences to be used in conducting a search.

Attributes

RPH	Uniquely identifies this origin destination information.The Reference Place Holder (RPH) is an index code used to identify an instance in a collection of like items (e.g. used to assign individual passengers or clients to particular itinerary items).
SameAirportInd	If true, the return departure must be from the same airport as the outbound arrival

Figure 5. Origin Destination Information (From OpenTravel, 2009b)

D. PUBLIC SECTOR DATA STANDARDS

Data standards are not only utilized in the aforementioned private sector examples, but also exist in the public sector as well. The public safety community, in particular the criminal justice community and the geospatial community in the United States, rely on data standards to enhance information

sharing. For the criminal justice community, NIEM has grown from being criminal justice specific to including other public safety exchanges. In addition, like the NIEM, the Federal Geographic Data Committee provides similar standards for government geospatial and mapping organizations.

NIEM**,** the data standard used in U.S. criminal justice, emergency management and intelligence fields, was built upon the Global Justice Extensible Markup Language (GJXML) data standard (partially shown in Figure 6). NIEM version 2.0 has expanded beyond public safety and criminal justice to include standards for emergency management, geospatial, immigration, intelligence, infrastructure protection, international trade, passenger and cargo screening, biometrics, and other customers (Bureau of Justice Assistance, 2007).

Person	**PersonType (SuperType)**	**Describes inherent and frequently associated characteristics of a person.**
PersonName	PersonNameType (SuperType)	A name by which a person is known.
PersonPrefixName	TextType	A title or honorific used by a person, e.g., Dr., Judge, General, Ms.
PersonGivenName	PersonNameTextType (TextType)	A first name of a person.
PersonMiddleName	PersonNameTextType (TextType)	A middle name of a person.
PersonSurName	PersonNameTextType (TextType)	A last name or family name of a person.
PersonSuffixName	TextType	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, (e.g., Jr, Sr, III), or otherwise qualifies the name (e.g., MD, LLD, PhD).
PersonMaidenName	PersonNameTextType (TextType)	An original surname of a person before changed by marriage.
PersonFullName	PersonNameTextType (TextType)	A complete name of a person.
PersonNameInitialsText	TextType	A first letter of a person's given, possibly middle, and last names.
PersonNameSoundexText	TextType	A name encoding such that similar sounding names with different spellings appear the same.
@personNameTypeCode	nonauth:PersonNameTypeCod	A code identifying a type of name for a person.
@personNameCommentText	xsd:string	A comment about a type of name for a person.
PersonAlternateName	PersonNameType (SuperType)	An alternate name used by a person. Sometimes referred to as an AKA.
PersonPrefixName	TextType	A title or honorific used by a person, e.g., Dr., Judge, General, Ms.
PersonGivenName	PersonNameTextType (TextType)	A first name of a person.
PersonMiddleName	PersonNameTextType (TextType)	A middle name of a person.
PersonSurName	PersonNameTextType (TextType)	A last name or family name of a person.
PersonSuffixName	TextType	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, (e.g., Jr, Sr, III), or otherwise qualifies the name (e.g.,

Figure 6. Global Justice Extensible Markup Language (GJXML) data standard (From U.S. Department of Justice, Office of Justice Programs, n.d.).

The Federal Geographic Data Committee (FGDC) creates data standards for U.S. government agencies for handling geospatial data. Figure 7 shows a segment of the FGDC's data standard for rail specific geospatial data. These standards allow the 28 federal agencies and departments to share information between their organizations, as well as with non-federal partners, such as state and local governments and private firms (Federal Geographic Data Committee, 2009). Each of these organizations requires different qualities in mapping and geospatial data, and these data standards allow for the differences. For instance, the Department of the Interior (DOI) is able to share data with the Environmental Protection Agency (EPA). The EPA may be interested in the water shed or runoff specifications of satellite data, while the DOI may be interested in the runoff specifications for an irrigation issue on an American Indian reservation. In this example, both organizations require geospatial data but for different reasons. These data standards allow these organizations to use one language when exchanging this information.

Line	Name/Role Name	Definition	Obligation Condition	Maximum Occurrence	Data Type	Domain
46	RailSeg	Linear section of a physical transportation system designed for railroad movement			<<Feature>>	Lines 47-65
47	owner	Person(s) or organization(s) that possess RailSeg	O	*	<<DataType>> OwnerInformation	Unrestricted
48	inServiceDate	Date the RailSeg was placed into service	O	1	Date	Valid historical or current date and time
49	outOfServiceDate	Date the RailSeg was taken out of service	O	1	Date	Valid historical or current date and time
50	isAlignment	Denotes whether or not the RailSeg is an Alignment	O	1	Boolean	True or False
51	isInService	Denotes whether or not the RailSeg is in service	M	1	Boolean	True or False
52	startingMileage	Mile at which the RailSeg begins	O	1	Number	Real Numbers
53	endingMileage	Mile at which the RailSeg ends	O	1	Number	Real Numbers
54	isFerry	Denotes whether or not the RailSeg represents a Ferry crossing	O	1	Boolean	True or False
55	Transportation Base:: TranSeg:status		M	1	CharacterString	Unrestricted
56	Transportation Base:: TranSeg::fieldMeasure		M	1	Measure	
57	Transportation Base:: TranSeg::length		M	1	Measure	
58	Transportation Base:: TranSeg::geometry	Shape and geolocation of a feature	O	*	<<Type>> GM_Curve	Defined in ISO 19107

Figure 7. Geographic Information Framework Data Standard for Rail Sector (From Federal Geographic Data Committee, 2013)

These private and public sector examples illustrate how data standards can enhance inter-organizational information sharing. In addition to data standards, process standards also assist in the sharing of information. These two standards complement one another—the data standards provide information-sharing partners with a standard language on what data elements will be shared, while process standards provide guidelines on how the data will be used.

E. PROCESS STANDARDS

Process standards are reliant on underlying data standards and came into being through a multi-organizational collaborative process to enhance inter-organizational information sharing further. Three such process standards, or protocols, are illustrated by the means of processing electronic mail, the communication of alerts and emergency announcements to the public, and the process of utilizing online travel sites for making online travel reservations.

Internet standards are formed as a result of the request for comment (RFC) process. The RFCs are reviewed and, if approved by a number of groups, become accepted standards for how the Internet will function. In August 1982, *RFC 821* was published (Postel, 1982). The subject of this particular RFC was Simple Mail Transfer Protocol (SMTP). This messaging exchange standard (revised many times since 1982) along with others like Post Office Protocol 3, better known as POP3, enable inter- and intra- organizational electronic mail exchanges. The data elements contained within the standards instruct the servers where to route messages (Postel, 1982). Another similar protocol is found in Common Alerting Protocol (CAP).

Government, as well as private organizations, use CAP to inform the public of on-going emergencies or emerging hazards. For example, weather-related alerts are authored using this protocol and the systems within media outlets (radio, television, Internet, etc.) automatically interrupt the broadcast and

supply the public the message (see Figure 8 for CAP data fields), which is performed without human interference or approval, rather via agreed upon process standards (Oasis, 2005).

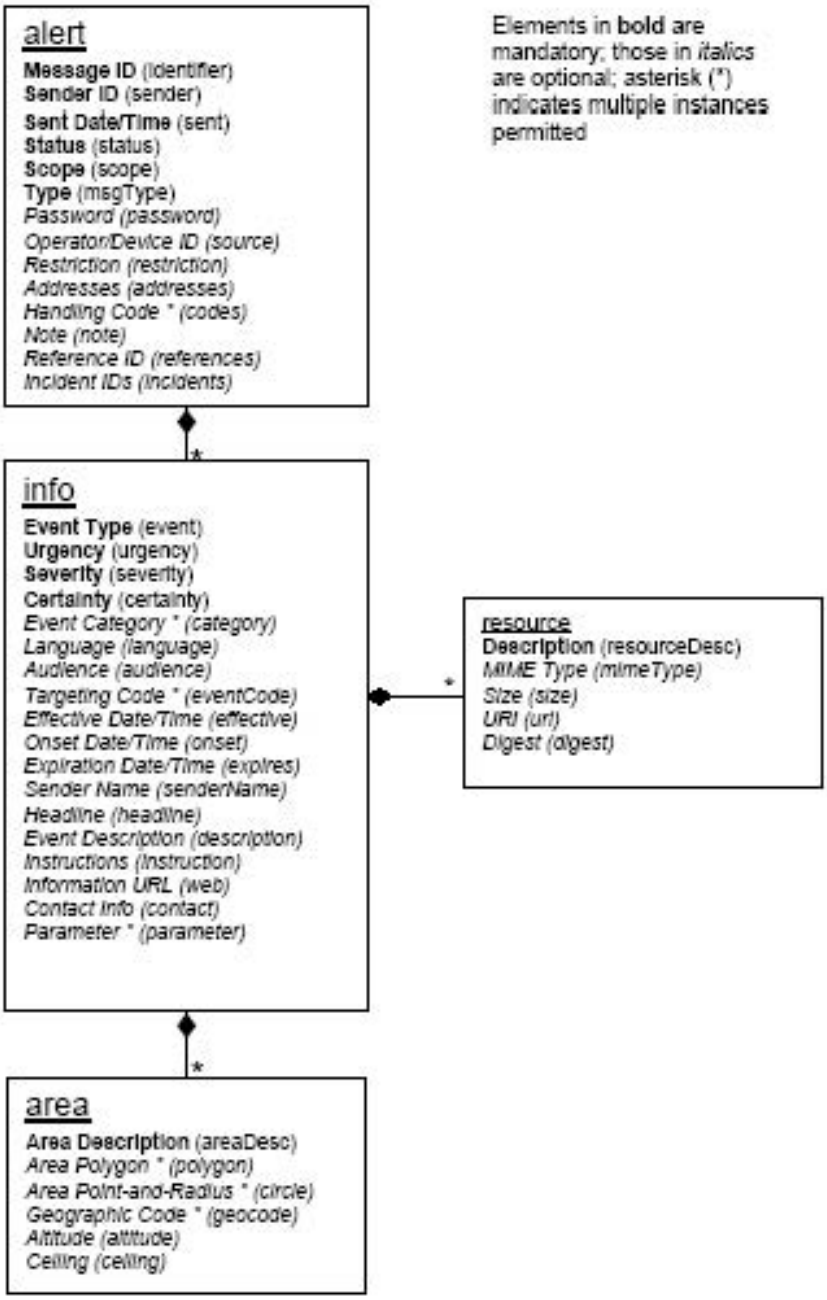


Figure 8. CAP data fields (From Oasis, 2010)

Another process standard, used by the OpenTravel Alliance's project, named FastRez, is illustrated in Figure 9. Using FastRez, the OpenTravel Alliance depicts how four processes (availability, reservation, reservation retrieval, and cancellation) are communicated between organizations. These processes enable hotels of any size to participate in information sharing between consumers, travel agencies, and online travel services (Open Travel, 2009a). Global Distribution Systems (GDS) is the name of the class of software utilized to facilitate information exchanges in the travel industry. These systems use process standards that allow information about a reservation, such as schedule, price, and accommodation types to be shared with travel agencies and travelers. Online consumer travel services, like Expedia.com, use GDS to communicate with hotels, airlines, and car rental companies (Radulović, 2013).

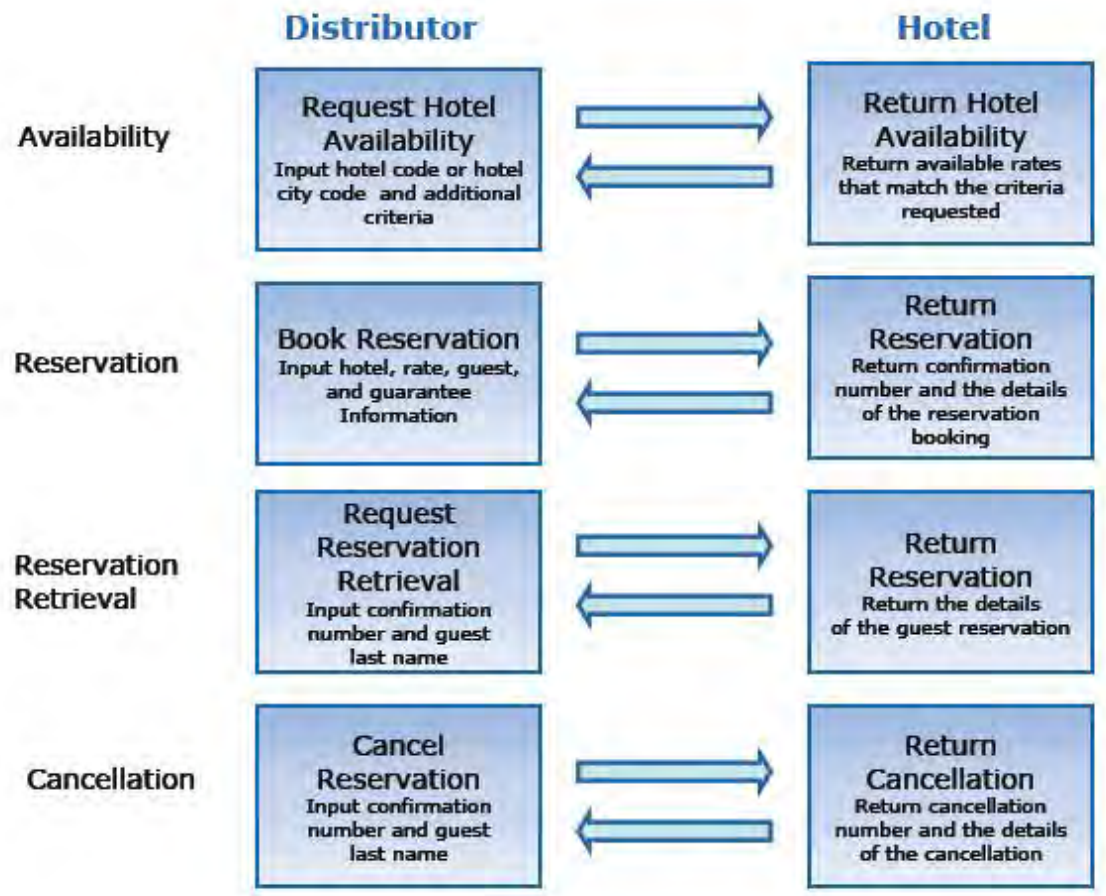


Figure 9. Open Travel Alliance—Fast Res System Flow (From Open Travel, 2009a)

Data and process standards allow both private and public organizations to use their intra-organizational tools while participating in inter-organizational information sharing. Information sharing tools are present in many industries to include those within the public sector. These tools can range from client-server applications to web-browser interfaces to shared data. Several of these tools are outlined in the next section.

F. PRIVATE SECTOR INFORMATION SHARING TOOLS

Private and public organizations have turned to technological tools to enhance inter-organizational information sharing. For the private sector, these tools can provide a gateway to B2B collaboration, and within government, these

tools enable sharing of information between agencies and departments. Some of these tools require a strong coupling between firms where two or more organizations use a common interface to exchange information on a particular project or product. Other information sharing tools are built to enable inter-organizational sharing by relying on data and process standards to govern information exchanges.

EDI has been used in inter-organizational information sharing, and in particular, within private sector supply chains. EDI is data and process standards based on information exchanges between partners (Dismukes & Godin, 1997). These exchanges are used to enable electronic exchanges between organizations on shipping, purchasing, payments, and other routine business processes (Attaran & Attaran, 2007). The Internet has improved EDI and reduced the necessary hardware from requiring a client server type solution to needing only a web browser (Attaran & Attaran, 2007). Some European travel and tourism organizations use an EDI to share information.

Based on data standards and an agreed business process, the Tourism Harmonisation Network (THN) provides a weak coupling between participants. Each organization supplies the availability of their resources to the THN and consumers or travel organizations can then query it based on their particular needs (Fodor & Werthner, 2004). Figure 10 graphically depicts the THN information-sharing model. In this structure, participants can use their in-house information management systems and still participate in a larger information-sharing network. Each participating organization shares a common set of data elements, which provide a common set of search or inquiry formats for the consumer. Fodor and Werthner (2004) write the following in their work on e-tourism and B2B collaboration in the marketplace.

> The philosophy is to allow participating organizations to retain their proprietary data formats and simultaneously cooperate with one other, exchanging information in a seamless manner. Participants receive data from their partners as if they were extensions of their own systems. (p. 16)

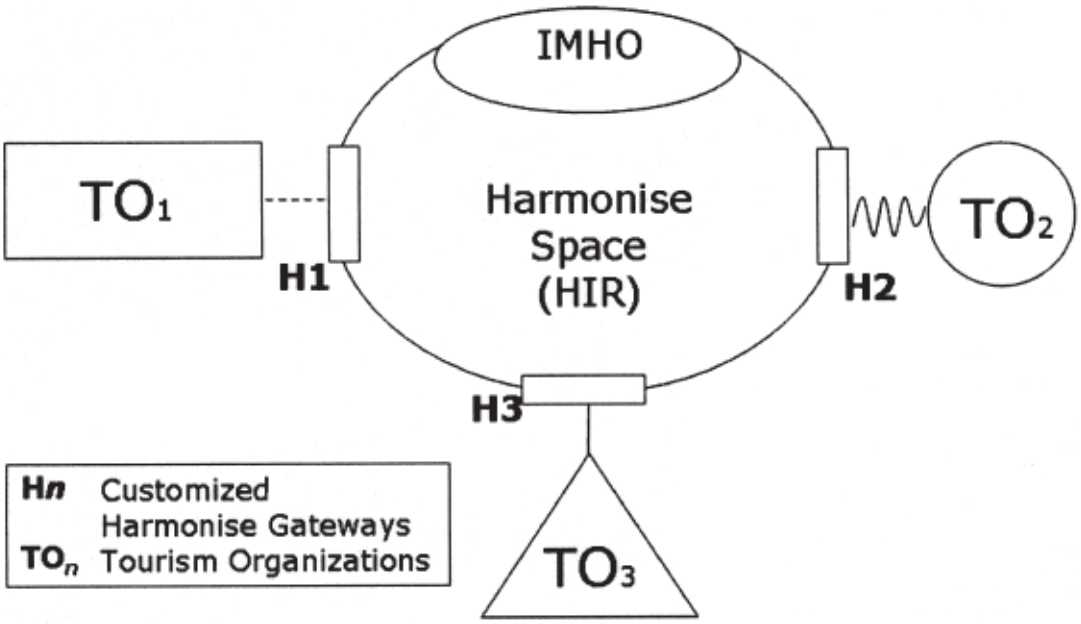


Figure 10. THN Information-Sharing Model (From Fodor & Werthner, 2004).

The travel industry uses a class of software called GDS and software suppliers have constructed tool sets to enhance information exchanges. Another example of a private sector information sharing tools in the travel and tourism industry is the Amadeus Cars solution. This tool, utilizing the data standards from OpenTravel Alliance, provides XML-based messaging for rental car providers (Amadeus, 2009). Amadeus, a private firm itself, provides this linkage to the travel and tourism industry. GDS suppliers Pegasus and WorldSpan supply tools to Expedia, which enable the traveler to search multiple airline, car rental and accommodation information simultaneously, based on the traveler's requirements (Expedia, 2013). These tools enable the sorting and filtering of results by price, schedule, provider, and other sometimes, other criteria. Another industry in which inter-organizational information sharing is paramount is the large retailer supply chain.

Some supply chains use tightly coupled inter-organizational information sharing tools. The CRP is one type of tool that two firms use to collaborate tightly. One example of a CRP system is the reordering process between a retailer and wholesaler. The two firms' inventory and ordering systems are linked

and automatically share information while acting upon pre-defined rules. Once the first order has been placed, terms have been agreed upon, and the inventory and ordering systems have been linked between firms, the CRP automatically shares information that results in the replenishment or reordering of the item (Attaran & Attaran, 2007). This system is an example of tightly coupled collaboration between firms and not only can be seen in the private sector, but also in the public sector.

G. PUBLIC SECTOR INFORMATION SHARING TOOLS

The public sector, in particular public safety organizations, uses inter-organizational information tools to enable sharing. Many of these tools are built on data and process standards. Some examples include the National Crime Information Center (NCIC), HSIN, and LEO.

1. National Crime Information Center (NCIC)

The NCIC is a computer-based database containing criminal justice records made available to law enforcement agencies nationwide. Examples of the information contained in these records include criminal histories, warrants, stolen property, and missing persons, just to name a few. Federal, state and local criminal justice agencies are able to populate the database, as well as make inquiries. Although the FBI maintains the host computer, the NCIC functions under a shared management concept, which includes other federal and state criminal justice agencies (U.S. Department of Justice, 2005). Operating procedures outlined in NCIC policy allow for system security and quality control.

2. Homeland Security Information Network (HSIN)

The HSIN brand is divided into two parts, HSIN and HSIN-Intel. The larger HSIN is devoted to information sharing within the public safety community, which includes law enforcement, emergency management, critical infrastructure, and others. The HSIN-Intel program serves the state and local fusion center community. Both programs are web portals with document libraries and

embedded communication capabilities. The portals are searchable, and in the HSIN-Intelligence portal, advanced storage abilities exist to limit document audience. In addition to document sharing, as well as secure messaging and chat, other features are also available. The HSIN offers a situational awareness tool called the COP and has integrated mapping capability through the iCAV. Both the COP and iCAV require the participating organization to login and enter their agencies' information into these unique portals.

3. Law Enforcement Online (LEO)

An initiative in the DOJ for information sharing is LEO. LEO operates similar to HSIN and provides some of the same functionality by offering secure messaging and mission specific online portals for communities of interest to post information. LEO's encryption package is used to verify users of other systems, such as N-DEx, and operational law enforcement deconfliction systems. In addition to web portals, LEO offers encryption for access to the national deconfliction network (RISSSafe) and VCC, which is a web-based incident management tool (U.S. Government Accountability Office, 2007).

H. CONCEPTUAL MODEL (NATIONAL INTELLIGENCE SHARING MODEL NISM)

Public safety organizations are constantly collecting information on situations, people, and places while performing their jobs. All too often, this information is stored inside an organization's data systems and not shared with peer agencies. The following model is built upon inter-organizational information sharing strategies from private and public organizations, and strives to improve information exchanges in the local, state, and federal arenas. As this literature explains, some of this work has already been accomplished, and provides a strong basis for the proposed model. For instance, some public sector data standards are in effect, and the NIEM and GJXML standards, are great

foundations upon which to build. Now, the standards already established must be applied to the domestic intelligence effort to enhance the RFI and situational awareness reporting processes.

The three elements outlined in this literature review (data standards, process standards, and information tools) are necessary for inter-organizational information sharing between domestic intelligence organizations. State and local fusion centers each have their own tools used for intra-organizational information sharing. Centers have databases, web portals, and other tools to share information within the center. Additionally, the centers are constantly processing information requests and since the data standards are in place, the next step is formalizing information sharing processes by modeling them after those used in the private sector among supply chains, for example.

This work focuses on four routine functions performed by state and local fusion centers: 1) request for information, 2) request for information reply, 3) situation report, and 4) situation report update. These four functions are detailed as follows in conceptual models.

I. FOUR CONCEPTUAL MODELS

The RFI model will consist of the following fields.

Organizational Information

- Agency, Fusion Center, etc.

Requestor & Contact Information

- Individual agent, officer, analyst, etc.
- Phone Number
- Email Address

Subject Biographical Information

- Name
- Date of Birth
- Social Security Number

Criminal Predicate

- Associated or suspected criminal activity

Narrative

- Brief background information

Sharing Controls

- Dissemination & Sharing Limits

Data Security Classification

- 28CFR
- For Official Use Only
- Law Enforcement Sensitive

Time Requirements

- Exigent
- Routine

The RFI reply model will consist of the following fields.

Organizational Information

- Agency, Fusion Center, etc.

Submitter Contact Information (if human processed)

- Individual agent, officer, analyst, etc.
- Phone Number
- E-Mail Address

Similar or Same Subject Biographical Information

- Name
- Date of Birth
- Social Security Number

Criminal Predicate

- Associated or suspected criminal activity

Narrative

- Brief explanation of information contained within the system

Sharing Controls

- Dissemination & Sharing Limits

Data Security Classification

- 28CFR
- For Official Use Only
- Law Enforcement Sensitive

The situation report model will consist of the following fields.

Organizational Information

- Agency, Fusion Center, etc.

Submitter Contact Information

- Individual agent, officer, analyst, etc.
- Phone Number
- Email Address

Situation Type

- Explosion, evacuation, suspicious activity, etc.

Original Jurisdiction

- Identity of local jurisdiction

Location

- Address & Coordinates

Persons Involved

- Deaths, Injured, Displaced, etc.

Narrative

- Brief background information

Sharing Controls

- Dissemination and Sharing Limits

Data Security Classification

- 28CFR
- For Official Use Only
- Law Enforcement Sensitive
- Open Source

The situation report update model will consist of the following fields.

Organizational Information

- Agency, Fusion Center, etc.

Submitter Contact Information

- Individual agent, officer, analyst, etc.

Situation Type

- Explosion, evacuation, suspicious activity, etc.

Original Jurisdiction

- Identity of local jurisdiction

Location

- Address & Coordinates

Persons Involved

- Deaths, Injured, Displaced, etc.

Narrative

- Brief background information

Status

- Continuing or Closed

Sharing Controls

- Dissemination and Sharing Limits

Data Security Classification

- 28CFR
- For Official Use Only
- Law Enforcement Sensitive
- Open Source

The data modules will be used in the following way.

The conceptual model, as depicted in Figure 11, shows how the flow of information is routinely processed by a state and local fusion center. These processes can take place many times each day.

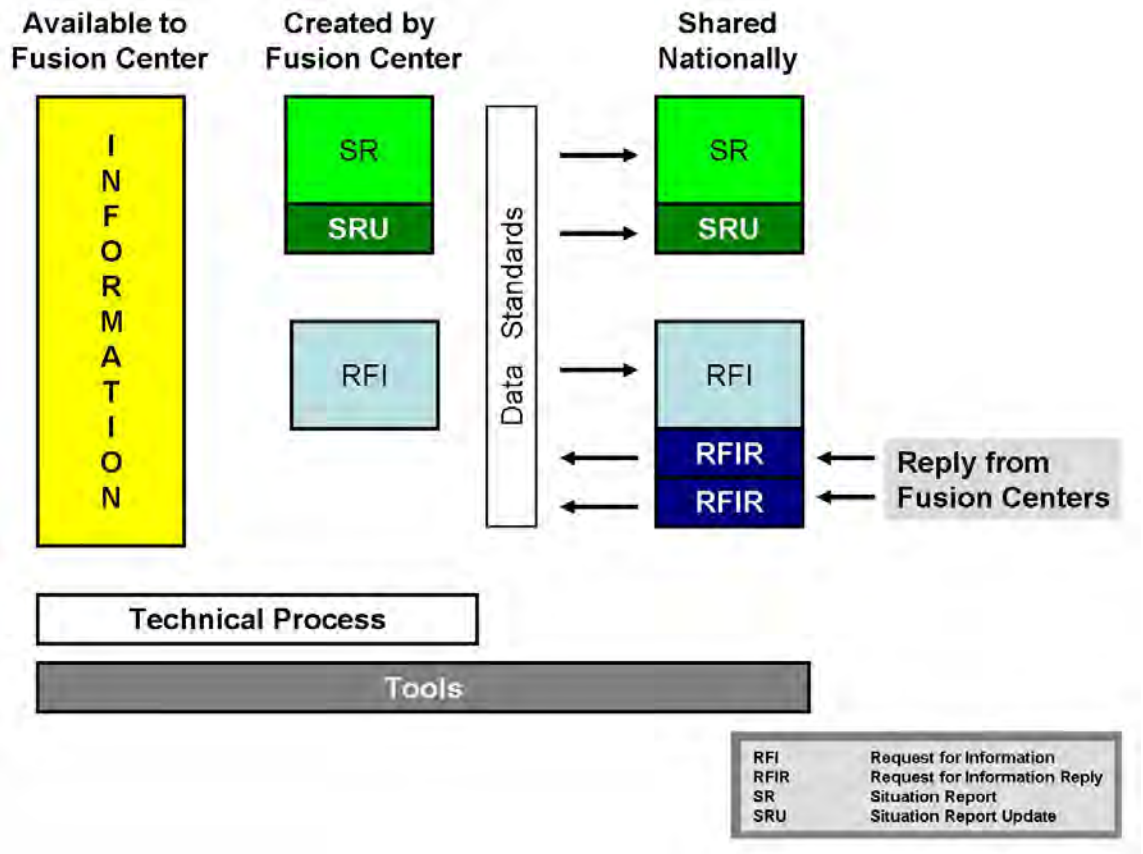


Figure 11. Conceptual Model

Using this model, the fusion center receives a RFI from a local police department on a subject who is suspected of being involved in criminal activity. The fusion center employee enters the call into the in-house system and begins searching databases available directly in the center. Using the established standards, the RFI is shared with the fusion center network and appears in each center's in-house systems as a new RFI regardless of what tools are being using to manage incoming requests. As these replies are received by the original center, they are threaded together under the original request. In addition to the RFI and RFIR processes, reporting on current situations is a routine fusion center function. In this example, a local emergency management organization reports to the fusion center that an aircraft has crashed in its jurisdiction, and it is responding to the crash site. This information is collected in the fusion center in-house information system, and when appropriate, is shared as situation reports with the other centers in the nation. These centers receive the information in their in-house system. When new information is received, such as fatalities or whether the aircraft is a commercial or pleasure, this information is shared using the same method as the original, and the updates append the original in the same way the RFIs are threaded together.

J. CONCLUSION

Data standards, process standards, and information-sharing tools are used in private and public organizations. Inter-organizational information sharing can benefit from these standards and tools. The public sector uses data standards to communicate criminal justice data and share geospatial information, and the private sector uses data standards to sell goods and share information with trading partners. Process standards are used in exchanging electronic mail and sharing public safety alerts. In addition to standards, information-sharing tools are used in public and private organizations. These tools are used in the travel and tourism industry, and inside supply chains. The public sector, in particular fusion centers, has information sharing tools like LEO and HSIN to aid in inter-organizational information sharing. This work builds on these standards

and tools to create a standards-based inter-organizational information sharing conceptual model for fusion centers to exchange RFI and situation reports. These routine fusion center business processes could benefit from this enhancement.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. METHODS

This thesis conducts a secondary analysis of the literature on data and process standards, and tools in the private and public sectors to build an idealized model, the NISM, or framework for conducting RFIs and providing situation reports. As set of evaluation criteria commonly used in the public and private sector was obtained from a group for SME. The author used those criteria along with existing literature to evaluate the proposed model. Between the literature available on private and public inter-organizational information sharing, a solid enough foundation is available to present a conceptual model. Coupling a literature review and interview validation process presents the best option for this project.

B. SAMPLE

The literature review includes scholarly journals on information technology, Internet sources, and websites. These sources were reviewed for publications and documentation on data standards, automated business processes, information sharing, and B2B information sharing. To validate the potential effectiveness of this model, qualitative interviews were conducted with individuals knowledgeable in the field of fusion centers. Interviews were conducted with an individual in a leadership position in the U.S. DHS Intelligence and Analysis Directorate, the former director of a mission-specific fusion center in the Defense Intelligence Agency, a state fusion center director, and a fusion center consultant from a technology firm.

C. DATA COLLECTION

Publications were gathered with relevance to data and process standards and information sharing tools. These publications exist in information science journals and public websites. The sources of the literature include industry

publications, studies on inter-organizational information sharing in private organizations, in particular supply chains, and government websites and publications. This literature was analyzed for application to the fusion center RFI and situation reporting process. Applicable concepts were included in the proposed model and provided to persons familiar with the U.S. fusion centers. The process consisted of conducting semi-structured interviews referencing the model to obtain feedback on the framework validity. Validity concepts include organizational and process fit. Based on those interviews, adjustments or modifications to the model are suggested.

D. ANALYSIS

Qualitative analysis of both the literature and interview data was performed to develop a model or framework for RFI and a national shared situational awareness. The results of the interviews were thematically mapped to enable the identification of common themes in the way of suggestions, comments, or other information gleaned from the interviews. These results were analyzed for inclusion into model adjustments or enhancements.

E. INTERVIEW QUESTIONS

Given the proposed conceptual model, the NISM, for enabling the fusion center RFI and situation reports business process, the following questions were asked:

Interview Question 1: Considering the NISM: How could public and private sector standards be leveraged to enhance the national distribution of situation reports and RFI's?

Interview Question 2: Considering the NISM: How could public and private sector processes, such as continuous replenishment programs in supply chains be leveraged to enhance the national distribution of situation reports and requests for information?

Interview Question 3: Considering the NISM: What is the role of tools in supporting domestic information sharing with respect to request for information processing and sharing situational awareness?

Interview Question 4: Would the NISM allow for more time for fusion centers to focus on strategic intelligence needs?

Interview Question 5: What challenges do you see in implementing such a concept?

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS / INTERVIEWS

Four SMEs were provided the conceptual model and an explanation of the use cases. Those interviewed included Van Godsey, the Missouri state fusion center director, Pat Duecy, the former director of the Defense Intelligence Agency (DIA) Joint Intelligence Task Force-Combating Terrorism (JITF-CT), Bart Johnson, the Principal Deputy Under Secretary within the (DHS) Intelligence and Analysis Directorate, and David Waldrop of Microsoft. Each of the participants was asked the same questions in the same order and several key themes were observed in their responses.

A. INTERVIEW QUESTIONS

The first question asked about the need for standards in processing RFIs and situation reports. The experts agreed that standards would be helpful and that trust was important to building information sharing systems. In particular, one interviewee commented that trust and strong relationships would be a prerequisite. The second question surrounded the use of process standards like those utilized by some supply chains for automatic reordering. Respondents felt that dissemination controls and information assurance would be concerns for implementation. The next question asked about the role of tools and each answer expressed the importance of tools. Some interviewees thought the information was too voluminous, while some thought too many disconnected tools were available. The fourth question assumes efficiencies in information exchanges would result in extra time for other duties, such as strategic intelligence. All respondents believed most of the work being done in a fusion center is tactical, and while one put a figure on the amount, another said little strategic thinking is happening. The last questions asked about the challenges for implementing the NISM. Participants felt two issues would be present, (1) skepticism, and (2) power and control issues.

Interview Question 1: Considering the NISM: How could public and private sector standards be leveraged to enhance the national distribution of situation reports and RFIs?

Two distinct themes emerged from the responses to the first interview question. To begin with, the answers expressed the necessity of data standards. Van Godsey, a state fusion center director, stated, “standards are important and vendors, contractors and information technology shops are accepting this” (personal communication, October 12, 2009).

Where the interviewees differed on this theme was in their feedback as to whether or not the public sector already has the appropriate framework for data standards. Two experts articulated that the public sector presently has standards in place for the model to utilize. One of these interviewees proposed the NIEM could be leveraged to enhance distribution. The other two experts suggested it is necessary to look to the private sector for ideas and guidance, and suggested that it may have already solved many of the information sharing problems faced by the public sector. Technology consultant and Microsoft employee David Waldrop commented that the data standards are not the first step but rather a necessity to enable technology (personal communication, October 14, 2009). He added that the standards should emerge and that it should not be assumed it could be designed (personal communication, October 14, 2009).

Pat Duecy, who formerly led counter-terrorism intelligence for the DIA, responded specifically that data standards for issues like naming fields of structured data fields are important. He added data standards should appear in both the RFI and situational reporting process (personal communication, October 13, 2009). Pat Duecy also stated that the people doing the work must lead the effort to explain the standard(s) for subsequent delivery to information technology personnel rather than the other way around (personal communication, October 13, 2009). Van Godsey built on this concept stating the user community would need to be very involved throughout such an implementation (personal communication, October 12, 2009). He continued the field names, whether they

are required or not, and issues like that would need to be discussed and approved by the organizations using the standards. Both Pat Duecy (personal communication, October 13, 2009), and Van Godsey (personal communication, October 12, 2009) commented if organizations already had an adopted data standard implemented, the homeland security community would be able to move the data more easily.

> Interview Question 2: Considering the NISM: How could public and private sector processes such as continuous replenishment programs in supply chains be leveraged to enhance the national distribution of situation reports and requests for information?

Process standards would be needed to implement the model (Van Godsey, personal communication, October 12, 2009).

As in the first question, all the experts believed a role existed for process standards, and specifically thought the concept of utilizing standards similar to CRP in supply chains could have merit in this construct. David Waldrop in the following narrative stated that automatic feed could be generated by the fusion center, and consumed by the fusion center for purposes of aggregating RFI and sharing situational reports (personal communication, October 14, 2009).

> Every partner who we have agreed to share information with is allowed access to our feed and vice versa. We would all agree to the rules of use for the information and agree on what information what shared etcetera. Like the first question on data standards the process standards would need the ability to evolve and adjust to the operating environment, changes in information, roles and other considerations.

Bart Johnson of the DHS I&A also mentioned that the process standards would create an assuredness that the information would be handled appropriately by all the organizations involved (personal communication, October 14, 2009). Pat Duecy said the process standards would first need to be agreed upon business rules by all organizations involved in the process (personal communication,

October 13, 2009). Then, they could be translated to rules within machines to aid in automating the process.

> Interview Question 3: Considering the NISM: What is the role of tools in supporting domestic information sharing with respect to request for information processing and sharing situational awareness?

In one way or another, all interviewees expressed the importance of information sharing tools in the model. “Tools allow the massive volume of information to be analyzed and allow data to be managed much, much quicker than a human mind,” (personal communication, October 12, 2009). Van Godsey. Van Godsey further stated that you “have to have tools,” and “tools can enable analysis through the use of timelines, link charts, mapping much quicker than the pace of a human” (personal communication, October 12, 2009). Also, tools allow for internal and external communication within, and between, agencies. The need for security and encryption tools was also expressed, as well as concerns regarding integration and confidence in the interviews. Bart Johnson suggested that one role for the tools would be to aid in the prioritization of information (personal communication, October 14, 2009). Since the tools are reading standards-based information, rules established could be established that route information, and alert organizations and individuals to specific issues. Pat Duecy built on this concept by adding the tools could help collate similar situational reports and show connections in information being exchanged (personal communication, October 13, 2009). Pat Duecy suggests that one key role for the tools would be to aggregate the information and visualize it in multiple fashions for the users (personal communication, October 13, 2009).

The distinct separation between the tools and the data standards allows for employing different sets of tools, but government agencies will not participate if tools are poorly integrated. The tools, specifically technology tools, are the enablers of the process standards as explained by David Waldrop’s expression, “just because you can buy an 18-volt Makita drill does not mean you can hang

kitchen cabinets" (personal communication, October 14, 2009). The drill will not hang the cabinets alone and possessing it will not make someone a craftsman, just as the information sharing tools are not actuating the information sharing; rather, they are facilitating its occurrence.

In addition to the apprehension of proper integration, confidence in the tools was also discussed. Agencies may question if communication issues will arise when an incident or situation is occurring, and must be certain these tools will handle all events without overloading the system. These agencies must also be confident that, in the event of numerous significant incidents developing in a short time period, the tools will "contribute to the solution, prioritization and handling of the information overload" as dictated by Bart Johnson (personal communication, October 14, 2009). Assurance has to be provided that the information and alerts are circulated, received, updated, and closed out; and tools can aid in that process.

Interview Question 4: Would this model allow for more time for fusion centers to focus on strategic intelligence needs?

A common denominator echoed in the respondents' answers is fusion centers spend a majority of their time and focus on tactical needs rather than intelligence needs. Van Godsey deducts "fusion center employees spend 80 to 85 percent of their time with tactical intelligence processing, while 15 to 20 percent of their time is dedicated to the strategic side" (personal communication, October 12, 2009). Pat Duecy stressed "very little strategic thinking and critical thinking is occurring. This type of thinking takes time and is almost impossible to accomplish in an atmosphere where in-boxes are constantly being filled" (personal communication, October 13, 2009). Thus, any procedure that takes away from the heavily sided tactical response, will add to any strategic needs. Both the above noted interviewees speculate the model would allow for more strategic intelligence requirements. However, this speculation also assumes the

processes and tools are allowing for the automation of generating and collating information sharing.

Although the model may permit increased strategic analysis, the increase could result in more hyper-tactical work. David Waldrop introduced this possibility in his comparison to the outcome of COP (personal communication, October 14, 2009). Crime rates escalated when COP was implemented due to the increased reporting of crimes as the police were being trusted more than before the incorporation of COP. It is possible all the extra time intended for strategic analysis would be spent sharing information and, in some ways, less time would be available. Furthermore, when the information really begins flowing, less time may be free for analysis of any kind.

Interview Question 5: What challenges do you see in implementing such a concept?

"This is the million dollar question," noted David Waldrop (personal communication, October 14, 2009). He continued, "Why are good ideas not implemented? The very entities of government are misguided," which was reflected in the answers of each interviewee. The experts identified several challenges that may materialize when attempting to administer the model. These potential impediments to implementation can be categorized under three main talking points: (1) overcoming skeptics, (2) issues of trust and relationships, and lastly, (3) power and control issues.

Firstly, as Van Godsey stated, "a lot of what we deal with now is skepticism, and these skeptics exist due to years of new systems being introduced " (personal communication, October 12, 2009). The mere mention of a new system generates feelings of suspicion and wariness. Personnel have become weary of new systems and databases largely because of broken promises and failed products. New systems were guaranteed to produce said results, and after implementation, were found to fall short of expectations, as

illustrated by Van Godsey's observation that "none of the federal government systems are producing what was intended" (personal communication, October 12, 2009). Additionally, some individuals will dislike the machine responses and prefer to review the information manually. This particular type of skepticism resonates with the trust issues discussed in previous answers and should be addressed with agreed upon data standards. Van Godsey added that adoption of the standard into everyday practice could be an additional challenge (personal communication, October 12, 2009). A last emerging issue, which revolves around skeptics, involves forming partnerships between agencies. According to Bart Johnson, "we do work well together and there is a need for a strong leader to force and form these partnerships. However, with the thousands of agencies and their thousands of protocols and procedures, we often revert back to the old school notion of not sharing information" (personal communication, October 14, 2009). This lack of sharing can result in hard feelings and damage existing partnerships, and force the process to start all over again. Cynics of the model may have experienced these failed partnerships and may caution moving forward.

B. ANALYSIS

As expressed above, respondents felt that this skepticism has led to low levels of trust and damaged relationships. A second issue, which emerged from the answers, centered on agency relationships. Regardless of data standards, local and state agencies must be involved and trust one another. One suggestion is to implement the model and standards first with adjoining states. Most local markets already work very well with each other and have established trust. David Waldrop asserted, "teams work together because they do not have to spell everything out every single time. They trust each other as a single unit. People knowing people is what works" (personal communication, October 14, 2009). Another interviewee stated the creation of fusions centers has been a positive step in the right direction. The model could first be attempted regionally where a recognized confidence between state fusion centers occurs, and then could

move outwards to connect centers across the nation eventually. Overall, the respondents believed that to be successful, mutual assurance must be established first, regardless of what standards are employed. Furthermore, the issue of trust reappeared in these answers. “There has to be information assuredness on both ends,” as stated by Bart Johnson (personal communication, October 14, 2009). Recognizing the information will be handled appropriately in regards to issues, such as controlling, sharing, and destroying, must be accepted. However, having agreed upon data standards may pave the way for trust in the processes. As noted by Waldrop, “the effectiveness is not whether or not we have a data standard, the magic is what happens on the other end.”

A third challenge to implementation articulated by the interviewed experts examines power and control issues. Questions regarding who will take a leadership role over the model were introduced. The respondents also recognized these problems might exist specifically between the federal government and state agencies in agreements over dissemination and content. Pat Duecy states, “there could be political influences to the practices” (personal communication, October 13, 2009). Potential solutions to these issues involve knowing and respecting the roles and responsibilities of each participating agency. “If the role is given to a federal agency, then the model may get bogged down versus giving the role to a small group of states for a regionally based pilot,” discussed Pat Ducey (personal communication, October 13, 2009). Additionally, those organizations that view themselves as aggregators of requests for information and situational reporting may fight for control, which slows down implementation even further. Power and control issues could also stem from the private sector and contractors. Numerous contractors have made their living by running and controlling other systems. These individuals may see this model as a threat. Likewise, existing information technology personnel may feel threatened by the possibility of being replaced or vie for control of the system. Specifically as noted by Bart Johnson, there are “too many tools and so many different contractors trying to sell something” (personal communication,

October 14, 2009). As such, David Waldrop suggests the types of tools in the model should not be forced upon the agencies (personal communication, October 14, 2009). Instead, existing tools or the agencies' choice of tools should be considered "so that as many people as possible can use the system," Waldrop explains (personal communication, October 14, 2009).

C. CONCLUSION

Overall, the four interviews provided some validation of the model, as well as some concerns not addressed by this work. Respondents felt trust could be a foundational issue with regard to the development of such a model, while skepticism about information-sharing programs has grown and could be another impediment. While the experts felt data and process standards were important, they believed information security and dissemination controls would be important to describe as well. All agreed that the majority of time spent in state and local fusion centers is focused on the tactical day-to-day operation, with not enough focus on strategic intelligence. Some thought integrated information-sharing tools could help create free time to address this imbalance.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

The following is a summary of the key findings from the analysis of the interviews.

A. DATA STANDARDS

Data standards should be constructed using a ground-up approach and be established by the user community.

The standards should include the fields necessary for exchanges between fusion centers, as well as name, date of birth and other biographical information.

The data standards should be built upon existing data standards, such as NIEM and GJXML.

B. PROCESS STANDARDS

Process standards would be necessary to implement the information exchange models.

Process standards would create assuredness between participating organizations that the information is handled appropriately.

The process standards could be found in the business rules of the organizations.

C. THE ROLE OF TOOLS

Tools would be necessary to analyze the information.

Tools can be used to aggregate information and aid in creating visualizations, such as link charts, timelines, maps, and others.

Tools could be used to alert organizations to specific types of information via a subscription service.

D. STRATEGIC WORK

The entire model would automate the process to the extent the analysts and fusion center staff could dedicate more time to other priorities, such as strategic intelligence and planning needs.

Efficiencies created by the model could create a new information overload problem for fusion centers that could have the reverse impact.

E. IMPLEMENTATION ISSUES

Need to overcome the skepticism that exists today among fusion center personnel who have been oversold and underdelivered with regard to information sharing initiatives.

Trust and damaged relationships would need to be a focus of a successful information-sharing implementation.

Power and control issues would need to be addressed prior to implementation.

F. RECOMMENDATIONS AND CONCLUSION

Nine years after 9/11, and six years since the 9/11 Commissioners released their recommendations, the nation is without a national intelligence sharing system. The Commissioners wrote:

> National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information. (National Commission on Terrorist Attacks, 2004)

It is the premise that "no one component [of government] holds all the relevant information," which has triggered the proliferation of information-sharing systems. Millions of dollars and several systems later an analyst at a state and local fusion center must either call or email a peer in a neighboring state or a distribution list in an attempt to gain the national knowledge on a subject or situation, which is not an efficient or effective way to share information. The private sector, presumably driven by efficiency and profits, has created several information-sharing models. Some of these models leverage data and process standards and information-sharing tools to enhance information sharing. Two routine functions of a fusion center are the processing of RFIs and sharing information about on-going situations. Each of these requires data exchanges with peer fusion centers and could be enhanced by employing the procedures used in the private sector.

Building a national information-sharing process for RFIs and sharing information about events would require interoperability. This interoperability is evidenced in private sector supply chains in which the individual firms use data and process standards to aid in the exchange of information between the firms and use information-sharing tools to interpret the information. The health care, real estate, and travel industries rely on the use of information exchange systems, such as EDIs, CRPs, or other types of middleware software to broker and route information. The use of CRPs is useful in automating routine information exchanges in which set rules or standards can be enforced by software. These information-sharing concepts could be transferred to the public sector to enable information sharing between domestic intelligence organizations, such as state and local fusion centers.

Interviewees said such an effort would require several key elements, such as strong relationships, trust, dissemination and security controls, data and process standards, and information-sharing tools. Only then would analysts have the time necessary to focus on the strategic intelligence needs of a state or local area. As cited in the review of the literature, researchers Cirincione and Bacharach (2007) state, “data standards represent agreement” (p. 136). Research indicates that data standards would be a necessary step to constructing an information-sharing system between state and local fusion centers, but a foundational phase of such work would be building trusting relationships between the organizations and people involved. State and local agencies must focus on building partnerships with the federal government, as well as agreeing on universal process standards, both of which require a joint effort between all agencies.

Pat Duecy said it best when he stated, “Business rules (i.e., policies) translate to machine rules” (personal communication, October 13, 2009). This concept is necessary for publishing and responding to the RFIs, as well as handling the dissemination of situation reports. For instance, rules on public disclosure and handling procedures for emerging incidents being reported using

this tool would need to be constructed and adhered to, as well as when an RFI can be distributed and what types of criminal activities are acceptable predicate offenses.

Information-sharing tools are being used by the private and public sector to share and process information. Such tools are necessary in the fusion center community. As Van Godsey emphasizes, “tools are important; they allow the massive volume of information to be analyzed” (personal communication, October 12, 2009). However, to do so, the various information-sharing tools employed by each fusion center must be integrated and allow for the importation and usage of standards-based data from other organizations.

One tool utilized by the private sector that automates routine information exchanges is known as CRP. This concept could be deployed to support the RFI processing. This technology would allow a fusion center employee to publish a RFI in Illinois. Then, the system would automatically collect the responses from all recipient centers, and allow each center to continue using the tools on which they are trained. The use of CRP systems builds on the pre-arranged data and process standards in the industry.

However, challenges exist in implementing this conceptual model to include overcoming skepticism, and understanding power and control issues. Several new information-sharing tools have been deployed in the domestic intelligence arena since 9/11, and while these tools have promised a lot of functionality and capabilities, they have not delivered. Overcoming the wide feeling of doubt that this implementation could actually be accomplished would be a considerable hurdle. Issues of who will be in charge of such a system, what systems it will “compete” with, funding, and others topics can derail even the best plan. Additional research could be conducted on some of these challenges, and on which past programs and projects have been successful.

G. FUTURE RESEARCH

Reponses in the interviews outlined other issues, which would require further research before the initiation of this concept. The need to understand the self-interest of organizational participation would be useful in creating a successful implementation. Understanding the implementation issues the private sector experienced during the development or deployment stages would be useful in mitigating them within the public sector. Researching the barriers and facilitators to building trust within similar networks would be a necessary foundational work. Considering the privacy and civil liberties issues would be necessary as local, state and federal statutes, policies and regulations regulate criminal intelligence information sharing. By addressing said issues, and continuing to research and experiment with various adaptations of private sector data and process standards and information-sharing tools, the public sector at the local, state, and federal levels can employ a more efficient means of sharing information and combating domestic and international crime threats.

H. PARTIAL IMPLEMENTATION

In December 2012, the Homeland Security State and Local Intelligence Executive Board proposed and accepted a portion of the situational awareness and RFI processing solution. This solution entailed utilizing a software already in use within the Homeland Security Information Network to create a virtual situational awareness workspace for the fusion center community to share information. Given that international terrorists have targeted elections in other countries, this communication method was tested on the U.S. national Election Day in 2012. Following the Election Day test and usage during some operational situations in Illinois, a conference call was conducted with several state fusion center directors who had recent experiences in major events. The fusion center directors from Colorado (selected because of the July 20, 2012 shooting at a theater in Aurora), Connecticut (reference the December 14, 2012 shooting at an elementary school in Newtown), and Oregon (selected because of the December

11, 2012, shooting at a mall in Portland) participated in the call and were surveyed about improving situational awareness reporting during an emerging or critical situation. These directors expressed interest in participating in a mechanism to share information with peer fusion centers and were encouraged about the positive influences this sharing could have on the network of fusion centers. The feedback from the personnel involved in recent critical incidents and the observations from the operational usage served as the foundation of the national situational awareness Adobe Connect site. The national situational awareness site or SitAware, as it is commonly referred, was used during the February 2013 Christopher Dorner manhunt investigation, and the April 2013 Boston Marathon Bombings (Figure 12). Both these events validated the need to improve information sharing between fusion centers. The full solution, as proposed in this thesis project, is not accomplished by the SitAware implementation.

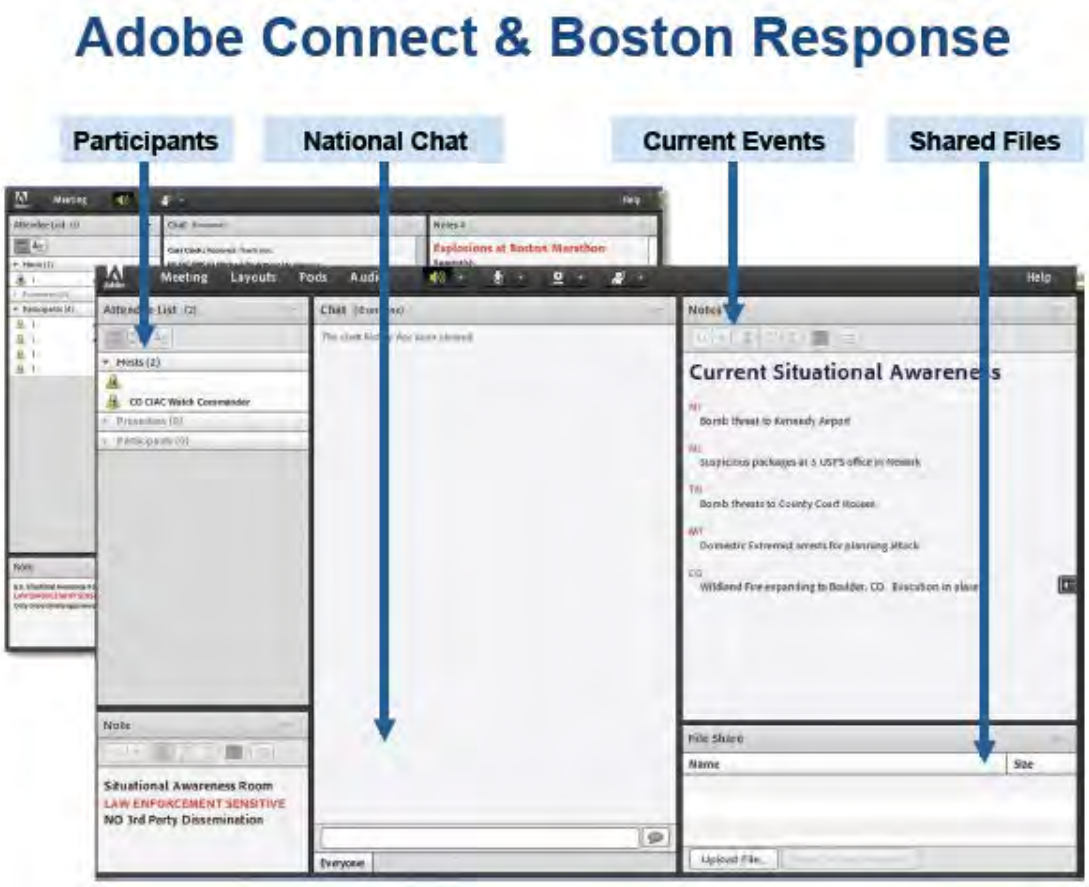


Figure 12. National Situational Awareness Connect Room—Boston Marathon Bombings, April 2013

The SitAware solution does not use a data standard approach to sharing information. Rather, it is reliant on each user posting information in the requested format, which creates situational awareness, and incomplete RFI messages (by comparison to the proposed data standard model) not in a standard format or appearance. The SitAware implementation does create an environment that fosters the fusion center community communicating more regularly, and especially, in a times of crisis. The SitAware environment was designed and the initial implementation was based on the three findings from this work.

During the interviews for this thesis project, the four SMEs expressed implementation concerns. The comments include the following.

Need to overcome skepticism due to a combination of overselling and under delivering of previous information-sharing solutions

Need to rebuild damaged trust relationship between the federal agencies and fusion centers

Need to address the authorities, access, and control of the system from the beginning.

Today's implementation of SitAware included information gathering and awareness briefings to the entire fusion center community to address the three issues identified. During implementation, other concerns were shared by the user community, and enhancements to the technology and policy will be considered in the upcoming months. Near-term additions to the SitAware site include the inclusions of a RFI template, geographic situational awareness software, and other administrative modules.

LIST OF REFERENCES

Attaran, M., & Attaran, S. (2007). Collaborative supply chain management. *Business Process Management Journal, 13*(3), 390.

Barratt, M. (2004). Understanding the meaning of collaboration in the supply chain. *Supply Chain Management: An International Journal*, *9*(1), 30–42.

Bureau of Justice Assistance. (2007, June). *Value of NIEM.* Retrieved from National Information Exchange Model website: http://www.niem.gov/pdf/ValueOfNIEM.pdf

Cirincione, J., & Bacharach, S. (2007). Data standards and service standards: helping businesses in real estate, mortgage, appraisal, and related industries function more efficiently. *Journal of Real Estate Literature, 15*(1), 127.

Department of Homeland Security. Office of Inspector General. (2013, June). *Homeland security information network improvements and challenges* (OIG-13–98). Washington, DC: GPO.

Dismukes, T., & Godin, P. (1997). International intermodal logistics, *Electronic Commerce World*, *7*(9), 46–8.

Expedia. (2013). *GDS hotels*. Retrieved from http://www.expedia.com/daily/home/vendor/gds.asp

Federal Geographic Data Committee. (2009). *Organization of FGDC*. Retrieved from http://www.fgdc.gov/organization

Federal Geographic Data Committee. (2013). *The federal geographic data committee.* Retrieved from http://http://www.fgdc.gov/

Fodor, O., & Werthner, H. (2004). Harmonise: A step toward an interoperable e-tourism marketplace. *International Journal of Electronic Commerce, 9*(2), 11.

Larence, E. R. (2011). *Statement for the record to the committee on homeland security and governmental affairs, U.S. senate. Information sharing. Progress made and challenges remaining in sharing terrorism-related information* (GAO-12–144T). Washington, DC: GPO.

Lefebvre, É., Cassivi, L., Lefebvre, L. A., & Léger, P. (2003). E-collaboration within one supply chain and its impact on firms' innovativeness and performance. *Information Systems and eBusiness Management*, *1*(2), 157.

National Association of Realtors. (2007). *What is a multiple listing service (MLS)?* Retrieved from Realtor.org

National Commission on Terrorist Attacks. (2004). *9/11 commission report*. New York: Norton.

National strategy for information sharing. (2007). Retrieved from Nationwide SAR Initiative NSI website: http://nsi.ncirc.gov/(S(kdyhncjxg2gklzboxcosmno4))/documents/National_Strategy_for_Information_Sharing.pdf

National Uniform Billing Committee. (n.d.). *UB92 claim form.* Retrieved from http://www.nubc.org/

Oasis. (2005, October). *Common alerting protocol, v. 1.1.* Retrieved from http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf

Oasis. (2010, July 1). *Common alerting protocol, v. 1.2, OASIS standard.* Retrieved from http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

OpenTravel. (2009a). *FastRez*. Retrieved from http://www.opentravel.org/FastRez/FAQ.aspx

OpenTravel. (2009b). *OpenTravel alliance message users guide.* Retrieved from http://www.opentravel.org/Specifications/SchemaIndex.aspx?FolderName=2009A

Postel, J. B. (1982, August). *Simple mail transfer protocol.* Retrieved from IETF Tools website: http://tools.ietf.org/html/rfc821

Radulović, L. (2013). The role and potential of global distribution system amadeus for tourism development at the global level. *Singidunum Journal, 10*(1), 28–38.

Real Estate Transaction Standard. (2009). *RETS*. Retrieved from http://www.rets.org/

U.S. Department of Justice. Office of Justice Programs. (n.d.). *Global justice XML (Archive)*. Retrieved from https://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1013

U.S. Department of Justice. (2005, September). *National crime information center, an overview*. Retrieved from Federal Bureau of Investigation website: http://www.fbi.gov/hq/cjisd/ncic_brochure.pdf

U.S. Government Accountability Office. (2007). *Information technology: homeland security information network needs to be better coordinated with key state and local initiatives* (GAO-07–822T). Retrieved from http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-07–822T/content-detail.html

U.S. Government Accountability Office. (2008). *Information technology — Management improvements needed on DHS next generation information sharing systems* (GAO-09-40). Washington, DC: GPO.

U.S. Government Accountability Office. (2010). *Report to congressional committees. Electronic personal health information exchange. Health care entities' reported disclosure practices and effects on quality of care* (GAO-10-361). Washington, DC: GPO.

White House, The. (2010). *White House National Security Strategy 2010.*

White House, The. (2012). *White House National Strategy for Information Sharing and Safeguarding 2012.*

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Amadeus. (2009, June 9). *Amadeus—The first travel distribution company to introduce XML messaging for car rental companies*. Retrieved from Amadeus http://www.amadeus.com/cars/x159673.html

American Hospital Association. (2009, 15 July). *Protocol*. Retrieved from National Uniform Billing Committee website: http://www.nubc.org/NUBC%20Protocol%20Approved%20July%2015,%202009.pdf

Carrillo Rivera, J. M. (2004). *Behavioral antecedents and strategic outcomes of inter-organizational collaborative capabilities* (dissertation). Concordia University, Canada.

Cassivi, L. (2006). Collaboration planning in a supply chain. *Supply Chain Management, 11*(3), 249.

Cassivi, L., Lefebvre, E., Lefebvre, L. A., & Leger, P. (2004). The impact of e-collaboration tools on firms' performance. *International Journal of Logistics Management, 15*(1), 91.

Chen, J., Tong, L., & Ngai, E. W. T. (2007). Inter-organizational knowledge management in complex products and systems. *Journal of Technology Management in China, 2*(2), 134.

Cheung, M. (2005). *Inter-firm knowledge sharing and its effect on relationship value: A global supply chain perspective* (dissertation). The University of Tennessee.

Engeström, Y., & Kerosuo, H. (2007). From workplace learning to inter-organizational learning and back: The contribution of activity theory. *Journal of Workplace Learning, 19*(6), 336.

Fahy, M., Feller, J., Finnegan, P., & Murphy, C. (2007). Complexity and context: emerging forms of collaborative inter-organizational systems. *JITTA : Journal of Information Technology Theory and Application*, *8*(4), 1.

Fawcett, S. E., Ogden, J. A., Magnan, G. M., & Cooper, M. B. (2006). Organizational commitment and governance for supply chain success. *International Journal of Physical Distribution & Logistics Management, 36*(1), 22.

Ford, N. J. (2006). The development and evaluation of an information technology support system to facilitate inter-organisational collaboration in HRD. *Journal of European Industrial Training*, *30*(7), 569.

Hadaya, P., & Pellerin, R. (2008). Determinants of manufacturing firms' intent to use web-based systems to share inventory information with their key suppliers. *International Journal of E-Collaboration*, *4*(2), 29.

Hartono, E. (2004). *Knowledge, technology, and inter-firm collaboration: A model and empirical study of collaborative commerce* (dissertation). University of Kentucky.

Hemphill, T. A. (2005). *Cooperative strategy and technology standards-setting: A study of United States wireless telecommunications industry standards development* (dissertation). The George Washington University.

Johnson, M. E., & Whang, S. (2002). E-business and supply chain management: An overview and framework. *Production and Operations Management*, *11*(4), 413.

Johnson, M. E., & Whang, S. (2002). Introduction to the special issues on e-business and supply chain management. *Production and Operations Management*, *11*(4), 411.

Kern, E., & Kersten, W. (2007). Framework for Internet-supported inter-organizational product development collaboration. *Journal of Enterprise Information Management*, *20*(5), 562.

Kock, N. (2008). International trade and world peace: The possible moderating effect of e-collaboration media naturalness. *International Journal of E-Collaboration*, *4*(2), I.

Kudaravalli, S., & Faraj, S. (2008). The structure of collaboration in electronic networks*. *Journal of the Association for Information Systems*, *9*(10/11), 706.

Kung, M. T., & Zhang, J. Y. (2008). Analysis of business process models in enterprise web services. *International Journal of E-Business Research*, *4*(2), 69.

Legner, C., & Schemm, J. (2008). Toward the inter-organizational product information supply chain—Evidence from the retail and consumer goods industries. *Journal of the Association for Information Systems*, *9*(3/4), 119.

Li, M., & Chen, H. (2008). Cross-national R&D collaboration: Determinants of governance of alliances and the effect of governance on technological innovation in science-based industry. *The Business Review, Cambridge*, *10*(1), 196.

Maccoby, M. (2006). Creating collaboration. *Research Technology Management*, *49*(6), 60.

McMurray, R. (2006). From partition to partnership: Managing collaboration within a curative framework for NHS care. *The International Journal of Public Sector Management*, *19*(3), 238.

Qureshi, S., Liu, M., & Vogel, D. (2006). The effects of electronic collaboration in distributed project management. *Group Decision and Negotiation*, *15*(1), 55.

Simatupang, T. M., & Sridharan, R. (2004). A benchmarking scheme for supply chain collaboration. *Benchmarking*, *11*(1), 9.

Tan, B. C. Y. (2007). Leveraging virtual communities for global competitiveness. *Journal of Global Information Management*, *15*(3), I.

Toiviainen, H. (2007). Inter-organizational learning across levels: an object-oriented approach. *Journal of Workplace Learning*, *19*(6), 343.

Travel Industry Wire. (2009, March 11). *OpenTravel alliance's fastrez(TM) cuts implementation time in half*. Retrieved from http://www.travelindustrywire.com/article37528.htmlhttp://www.realtor.org/law_and_policy/doj/mls_overview

Wang-Cowham, C. (2008). HR structure and HR knowledge transfer between subsidiaries in China. *The Learning Organization*, *15*(1), 26.

White, L. (2008). Connecting organizations: Developing the idea of network learning in inter-organizational settings. *Systems Research and Behavioral Science*, *25*(6), 701.

Whitford, J., & Zeitlin, J. (2004). Governing decentralized production: institutions, public policy, and the prospects for inter-firm collaboration in U.S. Manufacturing. *Industry and Innovation*, *11*(1/2), 11.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California